Install, Upgrade, and Maintenance Guide for Cisco Unity Connection

Release 10.x
Published November, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number:

Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 10.x

CONTENTS

1

Text Part Number:

CHAPTER 2

CHAPTER 3

CHAPTER 4

Preface

Audience and Use

The *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 10.x* explains the installation or upgrade scenarios of Cisco Unity Connection in various supported deployments. This guide also covers the steps for different migration scenarios, such as migrating a Cisco Unity server to a Unity Connection server and migrating a Unity Connection server running on a physical server to a virtual machine. In addition, this guide explains the procedure to take backup of a Unity Connection server using the supported tools.

Documentation Conventions

Table 1 Conventions in the Installation, Upgrade, and Maintenance Guide for Cisco Unity Connection

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Select **OK**.) • Information that you enter. (Example: Enter **Administrator** in the Username box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to https://<Cisco Unity Connection server IP address>/cuadmin.)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, select **Settings > Control Panel > Phone and Modem Options**.)

The *Installation, Upgrade, and Maintenance Guide for Cisco Unity Connection* also uses the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

(For translations of safety warnings listed in this guide, see *Regulatory Compliance and Safety Information for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/regulatory/compliance/ucwarns.html.)

Cisco Unity Connection Documentation

For descriptions and URLs of Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 10.x*. The document is shipped with Unity Connection Release 10.x, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/roadmap/10xcucdg.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Business Edition References in Documentation

In Unity Connection 10.x documentation set, all the references to "Cisco Business Edition" apply on Business Edition 6000/7000 only. The references do not apply on any other Business Editions.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. Using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Installing Cisco Unity Connection

Cisco Unity Connection can be deployed in either of the following ways:

- **Standalone Deployment**: Involves the installation of a Unity Connection as a single server.
- **Cluster Deployment**: Involves the installation of same version of two Unity Connection servers in an active-active or high availability mode. During the installation of Unity Connection as a cluster, the first server is referred to as publisher server and the second server as the subscriber server. For more information on cluster configuration, see the Configuring Cisco Unity Connection Cluster chapter.

Note Unity Connection 10.0(1) and later releases can only be installed on virtual machines. For more information, see the http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unity_Connection.

Methods of Installation

You can use either of the following methods to install standalone or cluster server:

- **Standard Installation**: Allows you to manually specify the installation information, such as hostname and IP address using installation wizard.
- **Unattended Installation**: Allows you to install Unity Connection using an installation disk and a pre-configured answer file floppy diskette. The answer file has all the information required for unattended installation. With Unity Connection 10.5(2) release, a seamless process of installation has been introduced, which allows you to start installation on both the publisher and subscriber servers simultaneously. The subscriber installation continues when the publisher is successfully installed. This type of unattended installation is Touchless Installation. For more information on Touchless Installation, see the Touchless Installation for Virtual Machine, page 1-18.

Note

- You can also perform fresh installation of Unity Connection10.x and later using Cisco Prime Collaboration Deployment. For more information on Cisco PCD, see http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.
- The answer file supports only fresh installs and does not support upgrades.

Important Considerations for Installation

Before you proceed with the installation, consider the following points:

- Verify the system requirements, such as licensing and phone integration requirements necessary for the Unity Connection server in the *System Requirements for Cisco Unity Connection* guide at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
- Be aware that when you install on an existing Unity Connection server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Ensure that you connect each Unity Connection server to an uninterruptible power supply (UPS) to provide power backup and protect your system. Failure to do so may result in damage to physical media and require a new installation.
- For a Unity Connection cluster:
  - Install the Unity Connection software first on the publisher server and then on the subscriber server (applicable to only standard installation scenarios). For more information on installation scenarios, see Installation Scenarios.
  - Note down the **Security** password that you mention at the time of installing publisher server. You need to specify the same password when installing the subscriber server in a cluster.
  - Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between the publisher and subscriber servers.
- Verify that DNS server is properly configured before installing Unity Connection. For more information, see the "Verifying DNS Settings" section on page 1-5.
- Do not perform any configuration changes during the installation.
- Be aware that the directory names and filenames that you enter during the installation are case-sensitive.

Pre-Installation Tasks

Before installing a Unity Connection server, you need to understand all the pre-installation steps as well. The Table 1-1 contains a list of pre-installation tasks that you must consider to ensure successful installation of Unity Connection server.

Table 1-1 Pre-Installation Tasks

	Task	Important Notes
Step 1	Ensure that your servers are listed as supported hardware and sized appropriately to support the load of the cluster.	For information about the capacity of server models, see the link http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unity_Connection.
Step 2	Create the virtual machine using the correct OVA template.	For more information, see the Creating a Virtual Machine, page 1-3 section.
Step 3	Change the boot order of the virtual machine to update the BIOS settings.	For more information, see the Changing the Boot Order of Virtual Machine, page 1-4 section.

Table 1-1 Pre-Installation Tasks

	Task	Important Notes
Step 4	Configure an external NTP server during a Unity Connection server installation. For a Unity Connection cluster, the NTP server helps to synchronize time between publisher and subscriber server. Ensure the external NTP server is stratum 9 or higher (meaning stratums 1-9). The subscriber server will get its time from the publisher server. To verify the NTP status of the publisher server, log into the Command Line Interface on the publisher server and enter the following command: **utils ntp status**	For more information, see the *Command Line Interface Reference Guide for Cisco Unified Solutions* for the latest release, available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html. ⚠ **Caution** If the publisher server fails to synchronize with an NTP server, installation of a subscriber server can also fail.
Step 5	Record the network interface card (NIC) speed and duplex settings of the switch port that connects to the new server.	Enable PortFast on all switch ports that are connected to Cisco servers. With PortFast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay [the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].
Step 6	Record the configurations settings for each server that you plan to install.	To record your configuration settings, see the Gathering Information for Installation, page 1-5 section.
Step 7	Download the signed .iso file of required Unity Connection version from Cisco.com.Upload it on a data store or burn a disk image of the downloaded software.	Download from the given link: http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm.

Creating a Virtual Machine

To download the OVA template for creating virtual machines, open the following link, select **Unity Connection Software**, and then select the appropriate release number:

http://software.cisco.com/download/type.html?mdfid=283062758&flowid=45673.

To Create a Virtual Machine:

Step 1 To deploy the OVA template in a supported VMware client, from the **File** menu, select **Deploy OVA template**.

Step 2 Next, browse the OVA template from the URL or file location on the system.

Step 3 Follow on-screen instructions to create the virtual machine.

Changing the Boot Order of Virtual Machine

To Change the Boot Order of the Unity Connection Virtual Machine

Step 1 In VMware client, power off the virtual machine that has the deployed OVA template.

Step 2 In the left pane of VMware client, right-click the name of the virtual machine, and select **Edit Settings**.

Step 3 In the **Virtual Machine Properties** dialog box, select the **Options** tab.

Step 4 In the **Settings** column, from the **Advanced** menu, select **Boot Options**.

Step 5 In the Force BIOS Setup, check the **The next time the virtual machine boots, force entry into the BIOS setup screen**. check box.

Step 6 Select **OK** to close the **Virtual Machine Properties** dialog box.

Step 7 Power on the virtual machine.

The virtual machine will boot into the **BIOS** menu.

Step 8 Navigate to the **Boot** menu and change the boot device order so the **CD-ROM** device is listed first and the **Hard Drive** device is listed second.

Step 9 Save the change and exit BIOS setup.

Changing Reservation on Virtual Machines Running with E7 or E5440 Processors

Added February, 2015

The CPU reservations are now included in OVAs, which are based on the Xeon 7500 processor. If the customer wants to run virtual machine on the E7 or E5440 processor, the CPU reservation numbers are higher than available cycles on 1 virtual CPU.

Based on the lab tests, we see that the 2.4 GHz reservation on E7 or E5540 processor has the same performance as a 2.53 GHz Xeon 7500 processor. Therefore, it is fine to change the reservation numbers on the virtual machine manually when running them on the E7 or E5440 processors for 5000, 10,000, or 20,000 deployment options.

For more on the reservations for the E7 or E5440 processor, see the docwiki available at http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unity_Connection.

To Change the Reservation Value of the Unity Connection 8.6(2) or Later Virtual Machine

Step 1 In VMware vSphere Client, select the host on which virtual machine is created.

Step 2 Click the **Summary** tab, under **CPU**, note the available CPU cycles for 1 virtual CPU in GHz.

Step 3 Power off the virtual machine on which you deployed the OVA template

Step 4 In the left pane of vSphere Client, right-click the name of the virtual machine and select **Edit Settings**.

Step 5 In the **Virtual Machine Properties** dialog box, select the **Resources** tab.

Step 6 In the **Settings** column, select **CPU**.

Step 7 Under **Resource Allocation**, enter the new reservation value in the **Reservation** textbox. The new reservation value is calculated as the number of CPUsX2.4GHz (for E5440 processor) and the number of CPUs multiplied by the 1 virtual CPU cycles in GHz (from step 2) (for E7 processor).

Step 8 Click **OK** to close the **Virtual Machine Properties** dialog box.

Step 9 Power ON the virtual machine.

Verifying DNS Settings

To Verify DNS Settings

Step 1 Login to command prompt.

Step 2 To ping each server by its DNS name, enter **ping** *DNS_name*.

Step 3 To look up each server by IP address, enter **nslookup** *IP_address*.

Gathering Information for Installation

Use the Table 1-2 to record the information about your server. Gather this information for a single Unity Connection server or for both the servers in a Unity Connection cluster. You should make copies of this table and record your entries for each server in a separate table.

Table 1-2 Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Installation?
Time Zone: ____________________	Sets the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your server. **Caution** In a cluster, you must set the subscriber server to the same time zone as the publisher server.	Yes, using the CLI command CLI > **set timezone**
MTU Size: _____________________	Sets the largest packet, in bytes, that this host will transmit on the network. By default, MTU is set to the size defined in the operating system. Selecting a different packet size would be more prevalent where a VPN or IPsec tunnel is used with a custom packet size. Web access over VPN can cause web pages not to load because of an improper MTU configuration. The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network. **Note** In clustered server pairs, the MTU setting must be the same on both servers.	Yes, using the CLI command CLI > **set network mtu**

Table 1-2 Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Installation?
Hostname and IP addresses: DHCP (Yes/No): ______ If DHCP is **No**: Hostname: _________________ IP Address: _________________ IP Mask: ___________________ Gateway (GW) Address:________	Sets whether to use DHCP to automatically configure the network settings on your server. If you select **No**, you must enter a hostname, IP address, IP address mask, and the gateway IP address. The hostname can contain up to 64 alphanumeric characters, hyphens, underscores, and period. The first character cannot be a hyphen. We recommend you use static Dynamic Host Control Protocol (DHCP) host configuration to ensure the DHCP server always provides the same IP address settings to the server **Note** If you do not have a gateway, you must still set this field to 255.255.255.255. Not specifying a gateway may limit you to only being able to communicate with devices on your subnet. **Caution** Make sure not to use **ciscounity** in the hostname of the server else enterprise replication will break.	Yes, using the CLI command CLI > **set network dhcp** CLI > **set network gateway** CLI > **set network ip eth0**
Domain Name Server: DNS: (Yes/No): ______ If DNS is **Yes**: Domain: ____________________ DNS Primary: _________________ DNS Secondary: _______________	Sets whether a DNS server resolves a hostname and IP address. **Note** Unity Connection enables the use of a domain name server to locate other Cisco Unity servers and devices. This is necessary when configuring digital networking and clustered server pairs. We recommend you to configure a secondary DNS server to avoid any loss of connectivity or service.	Yes, using the CLI commands CLI > **set network dns** CLI > **set network domain**

Table 1-2 Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Installation?
Administrator Account Credentials: Login: ___________________ Password: ________________	Sets the administrator credentials for secure shell access to the CLI and for logging into Cisco Unified Communications Operating System and Disaster Recovery System. The administrator account should be shared only with installers and engineers who have a thorough understanding and are responsible for platform administration and upgrades, and backup and restore operations. **Note** Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Login: No. Password: yes, using the CLI command CLI > **set password user admin** **Note** You can create additional administrator accounts after installation.
Certificate Information: Organization: ___________________ Unit: _____________________ Location: ________________ State: ___________________ Country: ________________	Sets information used by the server to generate certificate signing requests (CSRs) that are used to obtain third-party certificates. **Tip** To enter more than one business unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. For location, you can enter any setting that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, using the CLI command CLI > **set web-security**
Cluster: First server in cluster (Yes/No): ____ If First server is **No**: Publisher hostname: ___________ Publisher IP address: ___________ Publisher security password: ______	First server refers to the publisher server. During the installation of second or subscriber server, enter the details of the first server.	

Table 1-2 Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Installation?
NTP Servers: NTP Server 1: __________________ NTP Server 2: __________________ NTP Server 3: __________________ NTP Server 4: __________________ NTP Server 5: __________________	Sets the hostname or IP address of one or more network time protocol (NTP) servers that synchronizes with your Unity Connection server. The NTP service ensures that the time synchronized is accurate for date/timestamps of messages, reports, and various tools, such as logs and traces. All Unity Connection servers require an external NTP source that are accessible during installation. The source can be a corporate head-end router synchronized with a public NTP time server or it can be the public NTP time server itself. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v6. **Note** The NTP server that you specify for the publisher server is automatically applied for the subscriber server.	Yes, using Cisco Unified Operating System Administration: **Settings > NTP Servers** Using the CLI command CLI > **using the CLI command**
Security Password	Sets the password used by a subscriber server to communicate with a publisher server. The security password is also used by the Disaster Recovery System to encrypt backups. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.	Yes, using the CLI command CLI > **set password user security** **Caution** If you are changing the security password in a clustered server pair, you must change the security password on both servers and reboot both servers. For more information, see the description of this command in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Table 1-2 Gathering Information for Installation

Configuration Setting	Description	Can Setting Be Changed After Installation?
SMTP Server	Sets the hostname or IP address for the SMTP server that is used for outbound e-mail, intrasite links, Voice Profile for Internet Mail (VPIM), and HTTPS networking. The hostname can contain alphanumeric characters, hyphens, or periods but it must start with an alphanumeric character. **Note** You must specify an SMTP server if you plan to use electronic notification.	Yes, using the CLI command: CLI > **set smtp**
Application Account Credentials: Login: ____________________ Password: _________________	Sets the default credentials for the Unity Connection applications, including Cisco Unity Connection Administration and Cisco Unity Connection Serviceability.	Yes, using Cisco Unity Connection Administration and the CLI command: CLI > **utils cuc reset password**

Installation Scenarios

Table 1-3 Installation Scenarios

Installation Scenarios	Installation Method
Standalone Deployment	**Standard** • Installing the Publisher Server, page 1-12 • Verifying the Installation, page 1-22 **Unattended** • Generating Answer File for Unattended Installation, page 1-16 • Installing the Publisher Server, page 1-12 • Verifying the Installation, page 1-22
Cluster Deployment	**Standard** • Installing the Publisher Server, page 1-12 • Configuring Subscriber Server on the Publisher Server, page 1-15 • Installing the Subscriber Server, page 1-15 • Verifying the Installation, page 1-22 **Unattended** • Generating Answer File for Unattended Installation, page 1-16 • Installing the Publisher Server, page 1-12 • Configuring Subscriber Server on the Publisher Server, page 1-15 • Installing the Subscriber Server, page 1-15 • Verifying the Installation, page 1-22

Installation Tasks

Depending on the type of installation scenario, you need to perform the following tasks to install the Unity Connection software:

- Navigating Within the Installation Wizard, page 1-12
- Installing the Publisher Server, page 1-12
- Configuring Subscriber Server on the Publisher Server, page 1-15
- Installing the Subscriber Server, page 1-15
- Generating Answer File for Unattended Installation, page 1-16
- Touchless Installation for Virtual Machine, page 1-18
- Applying a Patch, page 1-19
- Verifying the Installation, page 1-22

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see Table 1-4.

Table 1-4 Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Select an option	Space bar or **Enter**
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or **Enter** to select **Back** (when available)
Get help information on a window	Space bar or **Enter** to select **Help** (when available)

Installing the Publisher Server

While installing a Unity Connection server, you are prompted to enter different configuration information. Refer the table mentioned in the Gathering Information for Installation, page 1-5 section wherever applicable.

To Install a Unity Connection Publisher Server

Step 1 Prepare the virtual machine to install Unity Connection:

a. Select **Edit virtual machine settings** to select the ISO image from CD/DVD drive using client device or from data store.

b. Navigate to the **Console** tab. A screen prompting you to check the integrity of the DVD appears.

c. Select **Yes** to perform the media check or **Skip** to move to the next step.

Note If you select media check and it fails, either download another copy from Cisco.com or obtain another DVD directly from Cisco.

d. After performing the hardware check, you get a prompt to restart the system. You need to select **Yes** to continue installation. After the system restarts, the **Product Deployment Selection** window displays.

Step 2 In the **Product Deployment Selection** window, select **Cisco Unity Connection** and select **OK**. The **Proceed with Install** window appears.

Step 3 In the **Proceed with Install** window, select **Yes** to continue the installation.

Caution If you select **Yes** on the **Proceed with Install** window, all existing data on your hard drive gets overwritten and destroyed.

The **Platform Installation Wizard** window appears.

Step 4 In the **Platform Installation Wizard** window, select the applicable option:

- If you want to perform a standard installation, select **Proceed**, and continue with this procedure.
- If you want to perform an unattended installation, select **Skip**. Connect the answer file image on a virtual floppy diskette and select **Continue**. The installation wizard will read the configuration information during the installation process and then follow the steps mentioned in the Post-Installation Tasks, page 1-24 section.

Step 5 If you select **Proceed** in the previous window, the **Apply Patch** window appears:

- Select **Yes** to upgrade to a later Service Release of the software during installation and follow the process mentioned in the Applying a Patch, page 1-19 section.
- Select **No** to skip this step and the **Basic Install** window appears.

Step 6 In the **Basic Install** window, select **Continue** to install the software version or configure the pre-installed software. The **Timezone Configuration** window appears.

Step 7 In the **Timezone Configuration** window, select the appropriate time zone for the server and then select **OK**. The **Auto Negotiation Configuration** window appears.

Caution In a cluster, the subscriber server must be configured to use the same time zone as the publisher server. The replication will not work if the timezone is not same.

Step 8 In the **Auto Negotiation Configuration** window, select **Continue**. The **MTU Configuration** window appears.

Step 9 In the **MTU Configuration** window, select the applicable option:

- Select **No** to accept the default value (1500 bytes).
- Select **Yes** to change the MTU size, enter the new MTU size, and select **OK.**

Caution If you configure the MTU size incorrectly, your network performance can be affected.

The **DHCP Configuration** window appears.

Step 10 In the **DHCP Configuration** window, select the applicable option:

- Select **Yes** to use DHCP server that is configured in your network.The network restarts and the **Administrator Login Configuration** window appears.
- Select **No** to configure a static IP address for the server and continue with this procedure. The **Static Network Configuration** window appears.

Step 11 In the **Static Network Configuration** window, enter the static network configuration information.

The **DNS Client Configuration** window displays.

Step 12 To enable **DNS**, choose **Yes**, enter the DNS client information and select **OK**.

The network restarts using the new configuration information and the **Administrator Login Configuration** window appears.

Step 13 Enter the administrator login and password.

The **Certificate Information** window appears.

Step 14 Enter your certificate signing request information and select **OK**.

The **First Node Configuration** window appears.

Step 15 In the **First Node Configuration** window, select the applicable option:

- Select **Yes** to configure this server as the publisher server or as a standalone server and continue this procedure. The **Network Time Protocol Client Configuration** window appears.
- Select **No** to configure this server as the subscriber server.

Step 16 In the **Network Time Protocol Client Configuration** window, enter the hostname or IP address of the NTP server(s) and select **OK**. The **Security Configuration** window appears.

Note Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher server. However, you can configure multiple NTP servers based on your requirements.

Step 17 In the **Security Configuration** window, enter the security password.

Note The system uses this password to authorize communications between the publisher and subscriber servers; you must ensure this password is identical on the two servers.

The **SMTP Host Configuration** window appears.

Step 18 In the **SMTP Host Configuration** window:

a. Select **Yes** to configure an SMTP server and enter the SMTP server name or IP address.

b. Select **OK**. The A**pplication User Configuration** window appears.

Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later using the platform GUI or the command line interface.

Step 19 In the **Application User Configuration** window:

a. Enter the Application User name and password and confirm the password by entering it again.

Note Do not use the system application name as the **Application User** name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database. The system application names are operator, replication, undeliverablemessagesmailbox, and Unity Connection.

b. Select **OK**. The **Platform Configuration Confirmation** window appears.

Step 20 In the **Platform Configuration Confirmation** window, select **OK** to continue the installation. The system installs and configures the software.

Step 21 When the installation process completes, you are prompted to log in using the Administrator account and password.

Step 22 Complete the post-installation tasks listed in the Post-Installation Tasks, page 1-24 section.

Configuring Subscriber Server on the Publisher Server

To Configure Subscriber server on the publisher server

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand **System Settings** and select **Cluster**.

Step 3 On the Find and List Servers page, select **Add New**.

Step 4 On the New Server Configuration page, in the **Hostname or IP Address** field, enter the hostname or IP address of the second server in the cluster.

Step 5 *(Optional)* In the **MAC Address** field, enter the MAC address of the second server.

Step 6 In the **Description** field, enter a description for the second server and select **Save**.

Installing the Subscriber Server

To install the subscriber server, follow the steps of installing publisher server until the **First Node Configuration** window appears and then continue the following procedure.

While installing a Unity Connection server, you are prompted to enter different configuration information. Refer the table mentioned in the Gathering Information for Installation, page 1-5 section wherever applicable.

To Install a Subscriber Server

Step 1 In the Console tab, on the **First Node Configuration** window, select **No** to continue the installation of the subscriber server and select **OK**.

The **Network Connectivity Test Configuration** window displays.

Step 2 During installation of a subscriber server, the system checks to ensure that the subscriber server can connect to the publisher server.

- To pause the installation after the system successfully verifies network connectivity, select **Yes**.
- To continue the installation, select **No**.

The **First Node Access Configuration** window displays.

Step 3 Enter the connectivity information for the publisher server and select **OK**.

The system checks for network connectivity.

If you select to pause the system after the system successfully verifies network connectivity, the **Successful Cisco Unity Connection to First Node** window displays. Select **Continue**.

Note If the network connectivity test fails, the system stops and allows you to go back and re-enter the parameter information.

The **SMTP Host Configuration** window displays.

Step 4 If you want to configure an SMTP server, select **Yes** and enter the SMTP server name.

The **Platform Configuration Confirmation** window displays.

Step 5 Select **OK** to start installing the software.

Step 6 When the installation process completes, you are prompted to log in using the Administrator account and password.

Step 7 Complete the post-installation tasks that are listed in the Post-Installation Tasks, page 1-24 section.

Generating Answer File for Unattended Installation

You can generate answer files using Cisco Unified Communications Answer File Generator web application. To use the answer file during installation, you need to save the answer file to the root directory of a floppy diskette, browse to the file during installation, and leave the installation to complete.

In case of Unity Connection cluster:

- You need to generate separate answer files for publisher and subscriber servers.
- You are not required to enter details of the publisher server manually on the subscriber server during subscriber server installation.

Note The Cisco Unified Communications Answer File Generator supports Internet Explorer version 11.0 or higher and Mozilla version 28.0 or higher.

Task List for Unattended Installation

You need to perform the following tasks to generate answer file and create floppy image for unattended installation.

1. Generate and download answer files that includes the *platformConfig.xml* files for both the publisher and the subscriber server. For more information on how to generate answer files, see To Generate and Download Answer Files using AFG, page 1-16.
2. After generating the answer files, create a floppy image. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739.
3. Deploy and configure the servers in the cluster, publisher and subscriber. For more information, see the To Configure the Publisher Server on Virtual Machine, page 1-17 and To Configure the Subscriber Server on Virtual Machine, page 1-17 section.
4. To install the publisher and subscriber server, see the Installing the Publisher Server, page 1-12 and Installing the Subscriber Server, page 1-15 section.

To Generate and Download Answer Files using AFG

Step 1 Log in to the Unity Connection Answer File Generator application. The answer file can be generated using the following link: http://www.cisco.com/web/cuc_afg/index.html.

Step 2 Enter details in the **Clusterwide Configuration** section.

Step 3 Enter details for the primary node in the **Primary Node Configuration** section.

Step 4 (Optional) If you want to enable Dynamic Cluster Configuration, enter a value in the **Dynamic-cluster-config-timer** field.

Note **Step 4** is mandatory when you are using Dynamic-cluster-configuration process for Touchless installation.

Step 5 Enter details for the secondary node in the **Secondary Node Configuration** section.

Step 6 In the **List of Secondary Nodes** list box, select **Add Secondary Node**. The node that you add as secondary node appears in this list box.

Step 7 Click **Generate Answer Files**. A dialog box appears showing the details for the primary node, the secondary node, and the clusterConfig file.

Step 8 In the **Communications Answer File Generator** dialog box, follow the download instructions, and then click the **Download File** button to download the answer files to your computer.

To Configure the Publisher Server on Virtual Machine

Step 1 Log in to the virtual machine to start the cluster installation.

Step 2 From the **VM** menu, choose **Edit settings** to mount the floppy image that you have created from the Answer File Generator tool. The **Virtual Machine Properties** dialog box appears.

Step 3 From the available hardware list, select **Floppy drive 1**.

Step 4 In the **Device Type** section, select **Use the existing floppy image in the database**, and then click **Browse** to navigate to the floppy image.

Step 5 Click **OK**. The floppy image is attached.

Step 6 Select the **CD/DVD Drive 1 > Connect to ISO image on local disk** option from the toolbar and choose **CD/DVD Drive1 > Connect to ISO image on a datastore**, navigate to the data store to select the ISO image, and click **OK**. The ISO image is attached and the installation starts.

Step 7 (Optional) If you want to test the media before the installation, click **OK** in the **Disc Found** message box, or select **Skip** to skip testing the media before the installation. The installation proceeds without any manual intervention. The publisher is installed and the subscribers is added to the publisher.

To Configure the Subscriber Server on Virtual Machine

Step 1 You can install the subscriber only after the publisher is installed.(Applicable to only unattended installation, not valid for Touchless install).

Step 2 Perform Step 1 to Step 6 of the To Configure the Publisher Server on Virtual Machine, page 1-17 procedure.

Touchless Installation for Virtual Machine

Touchless installation is an enhancement of the existing unattended installation, which promotes simplified cluster installation. In unattended installation, you first install Unity Connection on the publisher server using answer file, add the subscriber server to the **Cluster** page of the publisher server, and then start the installation of subscriber server. However, in Touchless installation, you are not required to manually enter the details of the subscriber server on the publisher server. The subscriber details are automatically updated through *clusterConfig.xml* file or *dynamic-cluster-configuration* option in the AFG tool, which minimizes the need for intervention and scheduling during the deployment of a new cluster.

Note *ClusterConfig.xml* file is generated only for the Touchless installation of Unity Connection 10.5(2) and above.

Methods for Touchless Installation

You can use either of the following two methods for Touchless installation:

- Predefined Cluster Configurations (AFG Process)
- Automatic Sequencing of Touchless server (Subscriber-Dynamic-Cluster configuration).

Predefined Cluster Configurations (AFG Process)

In this method of installation, the Answer File Generator (AFG) tool generates the *clusterConfig.xml* file along with the existing *platformConfig.xml* file for both the publisher and subscriber servers. If you specify the details of the subscriber server in the AFG tool, those details are included in the *clusterConfig.xml* file. After the publisher server is installed, it reads the *clusterConfig.xml* file and if the publisher server finds the subscriber server, it adds the subscriber server to its processnode table. Adding the subscriber server to the processnode table eliminates the need to wait for the publisher server to finish its installation, and then manually add the subscriber server on the server page.Thus, the entire installation process occurs automatically.

Automatic Sequencing of Touchless Server (**dynamic-cluster-configuration**)

In automatic sequencing feature, subscriber gets configured dynamically along with the publisher during the installation. To use this functionality, enable the **dynamic-cluster-configuration** option in the AFG tool or use the command line interface (CLI) command on the publisher server. To use CLI to enable dynamic-configuration functionality, see (Optional) To Enable Dynamic-Cluster-Configuration Using CLI, page 1-19. There is no *clusterconfig.xml* file in this process of Touchless install.You need to enable the Dynamic Cluster Config Timer (1-24 hours) and start the installation on both the servers at the same time. The number of hours is the duration for which subscriber waits for publisher to receive the subscriber entry in the processnode table.

Task List for Touchless Installation

You need to perform the following tasks to generate answer files and create floppy image for Touchless installation.

1. Generate and download answer files that includes the *platformConfig.xml* files for both the publisher and the subscriber server and clusterconfig.xml file (*only for* AFG Process). For more information on how to generate answer files, see To Generate and Download Answer Files using AFG, page 1-16.

Note In case you are using dynamic-cluster-configuration method of installation, then you just need to enable **dynamic-cluster-configuration** option in the AFG tool and follow the step1.

2. After generating the answer files, create a floppy image. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739.
3. Deploy and configure the servers in the cluster, publisher and subscriber. For more information, see the To Configure the Publisher Server on Virtual Machine, page 1-17 and To Configure the Subscriber Server on Virtual Machine, page 1-17 section.
4. To install the publisher server, see the Installing the Publisher Server, page 1-12 section for cluster deployment.
5. The installation of subscriber continues if:

- You enable the dynamic-cluster-configuration timer.
- The clusterConfig.xml files are present.

(Optional) To Enable Dynamic-Cluster-Configuration Using CLI

Step 1 You can enable Dynamic-Cluster-Configuration through the CLI for up to an hour using the command: set network cluster subscriber dynamic-cluster-config {default | no. of hours}. For more information, see the Set command chapter of *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)* guide at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/10_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100_chapter_0111.html#CUCM_CL_SD4F263F_00.

Step 2 Add the new cluster subscriber through the CLI in the following format: **set network cluster subscriber details** <servertype> <hostname> <ip> <domainname>.

Step 3 You can use **show network cluster** CLI to check the entries in the processnode table. For more information, see show command chapter of *Command Line Interface Guide for Cisco Unified Communications Solutions, Release 10.0(1)* guide at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/10_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100_chapter_0111.html#CUCM_CL_SD4F263F_00.

Applying a Patch

You must obtain the appropriate upgrade file from Cisco.com before you can upgrade during installation. To apply a patch, select **Yes** in the Apply a Patch window that appears during the installation of publisher or subscriber server. The installation wizard installs the software version on the DVD first and then restarts the system.

Note You can upgrade to any supported higher release if you have a full patch of the release not an Engineering Special (ES).

You can access the upgrade file during the installation process either from a local disk (DVD) or from a remote FTP or SFTP server.

To Apply a Patch

Step 1 If you select **Yes** in the Apply a Patch window, the **Install Upgrade Retrieval Mechanism Configuration** window appears.

Step 2 Select the upgrade retrieval mechanism to use to retrieve the upgrade file:

- **SFTP**—Retrieves the upgrade file from a remote server using the Secure File Transfer Protocol (SFTP). Skip to the Upgrading from a Remote Server, page 1-20 section.
- **FTP**—Retrieves the upgrade file from a remote server using File Transfer Protocol (FTP). Skip to the Upgrading from a Remote Server, page 1-20 section.
- **LOCAL**—Retrieves the upgrade file from a local DVD. Continue with the Upgrading from a Local Disk, page 1-22 section.

Upgrading from a Remote Server

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx. Cisco uses the following servers for internal testing. You may use one of these servers, but you must contact the vendor for support:

- Open SSH (for Unix systems. Refer to http://sshwindows.sourceforge.net/)
- Cygwin (http://www.cygwin.com/)
- Titan (http://www.titanftp.com/)

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

If you choose to upgrade through an FTP or SFTP connection to a remote server, you must first configure network settings so that the server can connect to the network.

To Upgrade from a Remote Server When Applying a Patch

Step 1 The **Auto Negotiation Configuration** window displays.

Step 2 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) using automatic negotiation. You can change this setting after installation.

Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To enable automatic negotiation, select **Yes**.

  The **MTU Configuration window** displays. Continue with Step 4.

- To disable automatic negotiation, select **No**. The **NIC Speed and Duplex Configuration** window **displays**. Continue with Step 3.

Step 3 If you choose to disable automatic negotiation, manually select the appropriate NIC speed and duplex settings now and select **OK** to continue.

The **MTU Configuration** window displays.

Step 4 In the **MTU Configuration** window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value.

⚠ **Caution** If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), select **No**.
- To change the MTU size from the operating system default, select **Yes**, enter the new MTU size, and select **OK**.

The **DHCP Configuration** window displays.

Step 5 For network configuration, you can choose to either set up static network IP addresses for the Unity Connection server and gateway or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended.

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The installation process attempts to verify network connectivity.
- If you want to configure static IP addresses for the server, choose **No**. The **Static Network Configuration** window displays.

Step 6 If you choose not to use DHCP, enter your static network configuration values and select **OK**.

The **DNS Client Configuration** window displays.

Step 7 To enable DNS, select **Yes**, enter the DNS client information and select **OK**.

After the system configures the network and checks for connectivity, the **Remote Patch Configuration** window displays.

Step 8 Enter the location and login information for the remote file server. The system connects to the remote server and retrieves a list of available upgrade patches.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path that starts with a drive letter (for example, C:).

The **Install Upgrade Patch Selection** window displays.

Step 9 Select the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system with the upgraded software version running.

After the system restarts, the **Pre-existing Configuration Information** window displays.

Step 10 To continue the installation, select **Proceed**.

The **Platform Installation Wizard** window displays.

Step 11 To continue the installation, select **Proceed** or select **Cancel** to stop the installation.

If you select **Proceed**, the Apply Patch window displays. Continue with Step 12.

If you select **Cancel**, the system halts, and you can safely power down the server.

Step 12 When the Apply Patch window displays, select **No,** the "**Basic Install**" window appears.

Step 13 Select **Continue** in the window to install the software version on the DVD or configure the pre- installed software and move to Step 7 of the Installing the Publisher Server section.

Upgrading from a Local Disk

Before you can upgrade from a local disk, you must download the appropriate patch file from Cisco.com and use it to create an upgrade DVD. You must create an ISO image on the DVD from the upgrade file. Just copying the ISO file to a DVD will not work.

To Upgrade from a Local Disk When Applying a Patch

Step 1 When the Local Patch Configuration window displays, enter the patch directory and patch name, if required, and select **OK**.

The **Install Upgrade Patch Selection Validation** window displays.

Step 2 The window displays the patch file that is available on the DVD. To update the system with this patch, select **Continue**.

Step 3 Select the upgrade patch to install. The system installs the patch, then restarts the system with the upgraded software version running.

After the system restarts, the Preexisting Configuration Information window displays.

Step 4 To continue the installation, select **Proceed**.

The **Platform Installation Wizard** window displays.

Step 5 To continue the installation, select **Proceed** or select **Cancel** to stop the installation.

If you select **Proceed**, the Apply Patch window displays. Continue with Step 6.

If you select **Cancel**, the system halts, and you can safely power down the server.

Step 6 When the Apply Patch window displays, select **No,** the "**Basic Install**" window appears.

Step 7 Select **Continue** in the window to install the software version on the DVD or configure the pre- installed software and move to Step 7 of the Installing the Publisher Server section.

Verifying the Installation

After the installation application has finished, the new server displays its hostname and the administration account login prompt.

To Verify the Installation

Step 1 Log in with the administration account user name and password.

The server opens a command line interface.

Step 2 Verify that server network services are running:

a. At the CLI prompt, enter the command **utils service list.**

It might take a few minutes for all services to start completely. During this time, you might notice that services might be listed as [Starting].

b. Repeat the **utils service list** command until all network services are listed as [Started].

In particular, the Cisco Tomcat service must be started before you can proceed to the next verification step.

Step 3 Verify the server details:

a. Open a web browser on a personal computer that has network access to the server. Unity Connection supports different web browsers, such as Microsoft Internet Explorer and Mozilla Firefox.

b. In the web browser, enter the URL "https://<*publisher_ip_address*>/cmplatform".

c. Login to Cisco Unified OS Administration using the *administrator* user name and password specified during the installation.

d. Select **Show > System** from the toolbar to display the system status page, showing the current date, uptime, software level, along with the CPU and memory usage.

e. Use the **Show** menu to check:

- **Cluster**: displays the IP address, hostname, alias, server type, and database replication status of the single server or both the server in case of cluster.
- **Hardware**: platform type, serial number, hardware, and other options
- **Network**: current network interface configuration, status, and packets
- **Software**: current active and inactive software partitions

Step 4 Verify the server status:

a. In the web browser, enter the URL "https://<*publisher_ip_address*>/cuadmin".

b. The Cisco Unity Connection Administration window opens. Select Cisco Unity Connection Serviceability from the navigation pane. Login using the *application* user name and password specified during the installation.

c. Select **Tools** > **Cluster Management**. It lists the server status of either single server or both the servers in case of cluster. For a standalone server deployment, the server shows **Primary** status whereas in case of cluster, one of the server shows **Primary** status and the other shows **Secondary** status.

Cisco Unity Connection Survivable Remote Site Voicemail Installation

You install a Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) server by converting a standalone Unity Connection server with the CLI command

utils cuc activate CUSRSV

Warning **After installing Unity Connection SRSV, you can not revert to a standalone Unity Connection server.**

Caution All the existing Unity Connection configurations are lost after running the conversion.

Note The unrestricted version of Unity Connection SRSV works only with the unrestricted version of Unity Connection (central) server.

Post-Installation Tasks

After installing Unity Connection on your server, you should perform the following additional tasks before configuring the system for your application:

- Obtain the licenses for the Unity Connection server.

  For more information, see the Managing Licenses chapter.

- *(Optional)* Change the application passwords.

  You can change the passwords using either the Cisco Unity Connection Administration web application, or you can log into the server and run the CLI command

  utils cuc reset password

- If you require additional languages, install them.

  For details, see the Adding or Removing Unity Connection Languages, page 5-9 section.

- Install the Cisco Unified Real-Time Monitoring Tool.

  You can use Cisco Unified Real-Time Monitoring Tool to monitor system health, and view and collect logs. For more information on RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide Release 10.x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/rtmt/CUCM_BK_CA30A928_00_cisco-unified-rtmt-administration-100.html.

  (*Optional*): You can configure RTMT to send alert notifications through emails to the specified email address. For more information on enabling email alert, see the "Enable email alert" section of the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

- Activate Unity Connection feature services.

  For service activation requirements, see the *Cisco Unified Serviceability Administration Guide Release 10.x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/serv_administration/guide/10xcucservagx.html.

- Configure the backup settings. For more information, see the Backing Up and Restoring Cisco Unity Connection Components chapter.

Troubleshooting Installation Issues

Follow the steps in this section to troubleshoot issues faced during installation.

- Examine the log files if you encounter problems during installation. Use the following commands in Command Line Interface to view log files.

  To obtain a list of install log files from the command line, enter

```
CLI>file list install *
```

To view the log file from the command line, enter

```
CLI>file view install log_file
```

where *log_file* is the log file name.

You can also view logs using the Cisco Unified Real-Time Monitoring Tool.

You can dump the install logs to the serial port of a virtual machine using the “Dumping Install Logs” procedure mentioned at http://docwiki.cisco.com/wiki/How_to_Dump_Install_Logs_to_the_Serial_Port_of_the_Virtual_Machine.

For more information on troubleshooting installation issues, see the *Troubleshooting Guide for Cisco Unity Connection Release 10.x,* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx.html.

Backing Up and Restoring Cisco Unity Connection Components

You must take the backup of Cisco Unity Connection components to avoid loosing any data or messages. The following are the tools supported for taking the backup or restoring the Unity Connection components:

- **COBRAS**, see the About COBRAS, page 2-1 section.
- **Disaster Recovery System**, see the About Disaster Recovery System, page 2-1 section.

About COBRAS

Cisco Unified Backup and Restore Application Suite (COBRAS) is an application used to migrate data and messages. You can take the backup using **Export** tool and restore the backup data using **Import** tool.

For more information, download the latest version of COBRAS, and view the training videos and **Help** at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

About Disaster Recovery System

The Disaster Recovery System (DRS) is web application that enables you to take the full backup of Unity Connection server components to remote locations using File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP).

You can take the backup of the following Unity Connection server components:

- Unity Connection configuration database
- Mailbox messages
- User greetings and recorded names
- Other server and platform components

DRS also provides a restore wizard that enables you to restore the Unity Connection server components from a backup file stored on an FTP or SFTP server.

Note You must configure the Unity Connection server with the settings similar to the server of which backup was taken before you can restore the software components.

All the tasks related to Cisco Unified Operating System Administration web interface remain in the locked state when Disaster Recovery System backup or restore is running. This is because DRS locks the operating system platform API. All the Command Line Interface (CLI) commands continue to work except for the CLI based upgrade command since the platform API is locked.

The Disaster Recovery System contains two key components:

- Master Agent (MA)
- Local Agent (LA)

The Master Agent coordinates the backup and restore activities with Local Agents. The system automatically activates both the Master Agent and the Local Agent on all the servers in the cluster.

Disaster Recovery System backup tasks can be configured from web interface or Command Line Interface (CLI) but configuring from web interface is more preferable. For information on configuring backup tasks using CLI, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*, *Release 10.0(1)*, available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/10_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100_chapter_01001.html#d3668e2997a1635.

Components Supported for DRS Backup

You can take the backup specific Unity Connection components. The components are listed under **Select Features**:

- **CUC**: Other Unity Connection server and platform components.
- **CONNECTION_GREETINGS_VOICENAMES**: All user greetings and recorded names.
- **PLM**: Unity Connection server licenses.
- **CONNECTION_DATABASE**: Unity Connection configuration database.
- **CONNECTION_MESSAGES_<*MAILBOXSTORENAME*>**: All messages in the named mailbox store.
- **CONNECTION_HTML_NOTIFICATION**: All HTML notification messages.

Note Selecting the **CONNECTION_GREETINGS_VOICENAMES** or **CONNECTION_HTML_NOTIFICATION** component automatically includes the **CONNECTION_DATABASE** component.

You should take the backup of all the server components when you are taking the backup for the first time, changing the backup device, upgrading the Unity Connection server to higher releases, migrating from physical server to virtual machine, or re-installing the server.

Backup Files in DRS

DRS stores the backup of all the server software components in multiple .tar files based on the component selected.

The .tar backup file includes an XML file called **drfComponent.xml** that contains a catalog of all the component files stored during the backup operation. When DRS performs the next backup operation, it uses the contents of this catalog to determine:

- Whether the number of .tar backup files should exceed the total number of backups you defined for the backup device.
- The .tar backup file to erase.

Caution DRS encrypts the .tar backup files using the security password configured during the installation of Unity Connection server. If you decide to change this password, perform a full DRS backup immediately. You must use the same security password on the replacement server when performing a restore operation.

Configuring DRS Backup

Note In a cluster deployment, you need to take the backup of publisher server only.

To Configure a DRS Backup

Step 1 **Set up and configure the FTP or SFTP server(s) used for storing the backups**.

A number of SFTP applications, such as FreeFTPd and Core FTP mini SFTP server are available that can be used to store and retrieve the backups.

To configure the FTP or SFTP server, you must define the directory that stores the backup and create an account that DRS can use to store and retrieve the backups.

Note Make sure there is enough capacity in the directory for the required number and size of backups. Keep in mind that the size of the backups will increase as the organization grows.

Step 2 **Configure a backup device in DRS**.

Each DRS backup device consists of the backup location, the FTP or SFTP account credentials, and the total number of backups that can be stored at the backup location. When the total number of allowed backups is reached, DRS overwrites the oldest backup on the server.

Follow the given steps to configure a backup device:

a. Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

b. Select **Backup**> **Backup Device**. The **Backup Device** window displays. Select **Add New**.

c. Enter the backup device name, network configuration information and the number of backups to store on network directory.

d. Select **Save** to create the backup device.

Note Depending on the backup policy and organization, it is advisable to create multiple backup devices for redundancy. If the organization consists of multiple locations, each location should have its own set of backup devices.

Caution Do not use the same network location/directory for different backup devices. Backup files for each Unity Connection server must be stored in a directory dedicated to that server.

Step 3 **Configure the backup process**

After creating the backup device, you can

- Configure a backup schedule using Configuring a Backup Schedule, page 2-4, or
- Configure a manual backup using Configuring a Manual Backup, page 2-5.

Configuring a Backup Schedule

You can create a different backup schedule for each backup device you created. Backup schedule can be configured to run the backup at different times. It is recommended to take multiple schedules, each stored on a different network location.

In most of the cases, you should set a schedule that performs a nightly backup during a defined maintenance window when there is the least amount of server and network traffic.

You can configure up to ten backup schedules, each has its own backup device, features, and components.

Note Disabling the schedule allows you to prevent the scheduled backups from running without deleting the schedule entirely.

To Configure a Backup Schedule for Each Backup Device in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup**> **Scheduler**. The **Schedule List** window displays.

Step 3 On the **Schedule List** window, select **Add New** to create a new backup schedule. The **Scheduler** window displays.

Step 4 On the **Scheduler** window, the following information are mentioned to configure a schedule:

- **Schedule Name**: Specify a schedule name.
- **Select Backup Device**: Specify the backup device for which you want to create a schedule.
- **Select Features**: Specify the Unity Connection components you want to backup.
- **Starts Backup at**: Specify the starting date and time of the schedule.
- **Frequency**: Specify the daily, weekly, or monthly cycles of the schedule.

Step 5 Select **Save** to apply the backup schedule.

Note If you select the **Set Default** option in the toolbar enables you to configure the backup schedule to perform weekly backups on Tuesday through Saturday.

Configuring a Manual Backup

You can run a manual backup for all components each time you create or change the configuration of a backup device.

Note Make sure to select all the components listed for backup.

The amount of time required to complete the backup depends on the size of the database and the number of components selected for backup. The maximum time taken for backup to complete is 20 hours or it will time out.

To Configure a Manual Backup in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup**> **Manual Backup**. The **Manual Backup** window displays.

Step 3 On the **Manual Backup** window,

- **Select Backup Device**: Specify the backup device to be used for backup.
- **Select Features**: Specify the Unity Connection components you want to backup.

Step 4 Select **Start Backup** to start the manual backup.

DRS generates a log file for each component after completing its backup. If an error occurred, you can open the component's log file to identify the specific error.

Viewing the Backup Status

To View the Backup Status in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup**> **Current Status**. The **Backup Status** window displays.

Step 3 The **Backup Status** window displays the current status of the components selected for backup.

Step 4 You can select **Cancel Backup** to cancel the backup after the backup of the current component completes.

Viewing the Backup History

To View the Backup History in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Backup**> **History**. The **Backup History** window displays.

Step 3 On the **Backup History** window, you can view the backup history after running a manual backup, to ensure it completed successfully.

Configuring DRS Restore

In case of Unity Connection cluster, you take the backup of publisher server only. Therefore, you need to restore only on the publisher server.

To Restore the Software Components on Unity Connection

Step 1 Install a new Unity Connection server.

The new server must be installed with exactly the same software and patches as the server being removed from service, and must be configured with the same hostname, IP address, and deployment type (standalone server or cluster pair). For example, the Disaster Recovery System does not allow a restore from version 8.5(**1**).1000-1 to version 8.5(**2**).1000-1, or from version 8.5(2).1000-**1** to version 8.5(2).1000-**2**. (The last parts of the version number change when you install a service release or an engineering special.)

Step 2 Follow the given steps after reinstalling Unity Connection:

a. Confirm that the IP address and hostname of the server matches the IP address and hostname of the server as it was before taking the backup.

b. Confirm that the following settings match the values when taking the server backups:

   - Time zone
   - NTP server
   - NIC speed and duplex settings
   - DHCP settings
   - Primary DNS settings
   - SMTP hostname
   - X.509 Certificate information (Organization, Unit, Location, State, and Country)

c. Confirm that the security password of the server matches the security password of the server as it was before taking the backup.

   DRS encrypts the backup data using security password as the encryption key. If you change the security password of the Unity Connection server after the last backup was taken, you need to enter the old security password during the restore process.

d. If any Unity Connection languages were previously installed, reinstall the same languages on the server.

Step 3 On the new server, log in to Disaster Recovery System (DRS) and recreate the backup device used to store the backups from the server removed from service. For more information on re-creating the backup device, see Configuring DRS Backup, page 2-3.

Step 4 Follow the given steps to run the restore operation in DRS:

a. Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

b. **Run the Restore Wizard**.

From the toolbar, select **Restore > Restore Wizard**.

c. Select the backup device you re-created and select **Next**.

d. Select the backup .tar file to restore the components and select **Next**.

Note DRS time stamps each backup file enabling you to easily select the backup file to use for a restore operation.

e. Select the software components to restore and select **Next**.

f. Select the specific server to restore each component.

Additionally, Unity Connection can perform a file integrity check as part of the restore operation. This is advisable to ensure that the files are valid and have not been corrupted during the backup or restore operations.

g. Select **Restore** to begin the restore of the selected .tar file to the server.

As with the restore operation, you can view the restore operation log file for each restored component.

Also as with a restore operation, the time it takes to restore depends on the size of the database and the components restored.

Step 5 Restart the new Unity Connection server. In case of a cluster server, reboot the publisher server.

Step 6 (*Cluster only*) Once the publisher reboots, run the following command on Command Line Interface (CLI) on the subscriber server to copy the data from the publisher to the subscriber server:

```
utils cuc cluster overwritedb
```

Step 7 (*Cluster only)* Run the following CLI command on either the publisher or subscriber server to check the status of the Unity Connection cluster:

```
show cuc cluster status
```

Verify that the status of publisher server is **Primary** and subscriber server is **Secondary**. Test and validate it before moving it back into production.

Viewing the Restore Status

To Check the Restore Status in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Restore > Current Status**. The **Restore Status** window displays.

The **Status** column in the **Restore Status** window shows the percentage of restore process completed.

Step 3 To view the restore log file, select the log filename link.

Viewing the Restore History

To View the Restore History in Disaster Recovery System

Step 1 Sign in to Disaster Recovery System and login using the same Administrator username and password that you use for Cisco Unified Operating System Administration.

Step 2 Select **Restore > History**. The **Restore History** window displays.

Step 3 On the **Restore History** window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

Note The **Restore History** window displays only the last 20 restore jobs.

CHAPTER 3

Upgrading Cisco Unity Connection

You need to upgrade from the current version of Cisco Unity Connection to a higher version to use the new features supported with the new version. When you upgrade a server, the new version of Unity Connection is installed in a separate disk partition known as inactive partition. To activate the new version, you need to perform switch version. The following are the two ways to switch to the new version:

- **Automatic Switching**: Allows you to automatically switch to the new version of Unity Connection as part of the upgrade process.
- **Manual Switching**: Allows you to manually switch to the new version of Unity Connection after the successful completion of upgrade.

If you need to revert the server to the previous version, you can rollback to the previous version.

Note You can install or upgrade Unity Connection 10.0(1) and later releases only on virtual machines.

Upgrade Types

The Unity Connection upgrade files are available as ISO images or COP (Cisco Option Package) files. You can use either of the following interfaces to upgrade Unity Connection:

- Command Line Interface (CLI)
- Cisco Unified OS Administration web interface.

You must save the COP files on a Network Location FTP/SFTP server accessible during upgrade. ISO image can be saved on a local DVD or on a network location. The performance of the upgrades can be monitored through CLI or Cisco Unified Operating System Administration interfaces.

The Table 3-1 explains the upgrade types and supported upgrade paths from one version to another.

Table 3-1 Upgrade Matrix for Unity Connection

Upgrade Type	Upgrade Path	Description
Service Update (SU)	Examples of supported paths: • 10.5.x/10.5.xSUx1 to 10.5.xSUx2 • 8.6.x/8.6.xSUx1 to 8.6.xSUx2	• SU is installed on the inactive partition to which you can switch later on. • ISO images are non-bootable images not meant for installation.
Refresh Upgrade (RU)	8.5 or earlier to 10.x or later	• If the RHEL version of the Unity Connection operating system changes during an upgrade, it is referred to as a Refresh Upgrade (RU). • You need the following COP files before performing this upgrade: – ciscocm.refresh_upgrade.cop – ciscocm.version3-keys.cop • The new version is installed on the inactive partition. You should perform automatic switch version during RU for successful upgrade.
	9.x.x or earlier to 10.x or later	• You need the following COP file before performing this upgrade: – ciscocm.version3-keys.cop • The new version is installed on the inactive partition. You should perform automatic switch version during RU for successful upgrade.
Level 2 (L2)	Examples of supported paths: • 10.0.x to 10.5.y • 10.5.x to 10.5.y • 9.x to 9.y	• If the RHEL version of the Unity Connection operating system do not change during an upgrade, it is referred to as an Level 2 (L2) upgrade. • The new version is installed on the inactive partition to which you can switch later on.
COP file, for more information, see the Applying COP file from a Network Location, page 3-9 section.	Fix for the same version	• COP files are installed on the active partition and you cannot uninstall them. Contact Cisco TAC to uninstall COP files.

Note After the upgrade, you may need to reinstall the locale depending on the source and the target version. If the target version is compatible with the existing locales, then you need not install any new locales. However, if the target version requires to install new locales, then first verify the existing locales using the CLI **show cuc locale**, remove the existing set of locales after the completion of upgrade process, and install the new set available locales. If there is no set of available locales with the target version, then simply install the new set of locales.

Status of Unity Connection Cluster During L2 Upgrade

When Unity Connection is upgraded, then during switch version the subscriber server continues to provide services to users and callers. However, the performance of the cluster is affected in the following ways:

- If the phone system is routing calls to the subscriber server, outside callers and Unity Connection users can leave voice messages but the messages are not immediately delivered to user mailboxes. During switch version on the subscriber server in a cluster, messages that were left on the subscriber server are copied to the publisher server and delivered to user mailboxes.
- Unity Connection users can use the telephone user interface (TUI) to play messages recorded before the upgrade starts but cannot play the messages recorded during the upgrade.
- Unity Connection may not retain the status of messages. For example, if a user plays a message during the upgrade, the message may be marked as new again after the upgrade. Likewise, if a user deletes a message during the upgrade, the message may reappear after the upgrade.
- During an upgrade, users can access Unity Connection using clients, such as ViewMail for Outlook and Web Inbox other than the telephone user interface (TUI). During the switch version, publisher will display “message could not be loaded” for web inbox. The subscriber is completely disabled during the switch version.
- Administrator users can make configuration changes using any of the administration applications, such as Cisco Unity Connection Administration and Cisco Unified Operating System Administration since the administration applications are disabled for both publisher and subscriber during an upgrade. The configuration changes cannot be made during the switch version.
- Intrasite, intersite or HTTPS networking with other servers is disabled for the duration of the switch version. Directory changes made on the other servers in the network are not replicated to the server or cluster until the switch version is complete.

Note You can also upgrade Unity Connection 10.x and later using Cisco Prime Collaboration Deployment. For more information on Cisco PCD, see http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.

Status of Unity Connection Cluster During RU

During the refresh upgrade, the publisher server is completely disabled for the entire duration of upgrade but the subscriber server continues to provide services to users and callers.

- If the phone system is routing calls to the subscriber server, outside callers and Unity Connection users can leave voice messages but the messages are not immediately delivered to user mailboxes. During switch version on the subscriber server in a cluster, messages that were left on the subscriber server are copied to the publisher server and delivered to user mailboxes.
- Unity Connection users can use the telephone user interface (touchtone conversation) to listen to messages that are left before you start the upgrade. However, users cannot listen to messages that are left during the upgrade. But can access those messages after both the servers in the cluster are successfully upgraded.
- Unity Connection may not retain the status of messages. For example, if a user plays a message during the upgrade, the message may be marked as new again after the upgrade. Likewise, if a user deletes a message during the upgrade, the message may reappear after the upgrade.
- During an upgrade, users can access Unity Connection using clients, such as ViewMail for Outlook and Web Inbox other than the telephone user interface (TUI). During the upgrade, publisher will display “message could not be loaded” for web inbox.
- Administrator users cannot make configuration changes using any of the administration applications, such as Cisco Unity Connection Administration and Cisco Unified Operating System Administration since the administration applications are disabled for both publisher and subscriber during an upgrade.
- Intrasite, intersite or HTTPS networking with other servers is disabled for the duration of the upgrade. Directory changes made on the other servers in the network are not replicated to the server or cluster until the switch version is complete.

Duration of Upgrade

Under ideal network conditions, an upgrade process takes approximately two hours to complete on each server. Therefore, a Unity Connection cluster takes four hours to upgrade to a higher version. Depending on the data size of the server, the switch version process might take some more time.

If you are upgrading in a slow network condition, the upgrade process may take longer time than expected. It is always recommended to upgrade Unity Connection during off-peak hours or during a maintenance window to avoid service interruptions.

Tip You can reduce the duration of upgrade process by asking users to permanently delete items in the deleted items folder before starting the upgrade. This saves time as deleted items will not be copied.

Prerequisites for Upgrade

Before beginning the upgrade process, you must consider the following points for a successful upgrade:

- Ensure that you have a good network connection to avoid service interruptions during upgrade.
- You must have a Secure File Transfer Protocol (SFTP) or File Transfer Protocol (FTP) server in place when upgrading from a network location.
- Check the current version and determine the version to which you want to upgrade. See the release notes of the new version for more information. Release notes are available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.

- Determine if you need COP files depending on the upgrade process. Download the COP and ISO image files from:

  http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm.

- Backup all the existing data. For more information on backup and restore, see the Backing Up and Restoring Cisco Unity Connection Components chapter.
- Confirm that the status of both publisher and subscriber servers is active and they can answer calls. Follow the given steps to confirm the server status in a cluster:
  - **a.** Sign in to Cisco Unity Connection Serviceability.
  - **b.** Expand **Tools** and select **Cluster Management**.
  - **c.** Check the server status in a cluster.
  - **d.** In addition to this, confirm the running state of database replication using the CLI command **show cuc cluster status.**

Note After confirming the status of publisher server as **Primary** and subscriber server as **Secondary**, start the upgrade process first on publisher server and then on subscriber server.

- Initiate a pre upgrade test before starting the upgrade process using the CLI command

  run cuc preupgrade test

Warning **If you are upgrading from Unity Connection 8.6 or earlier, you must install all the applicable licenses before you upgrade to Unity Connection release 9.x and later. This is because the installed license information considered as legacy license data is required to migrate licenses. After you upgrade to Unity Connection 9.x and later releases, you can not apply legacy licenses using the Prime License Manager. For more information see the Migrating Licenses from Unity Connection 8.6 and Earlier Releases, page 6-3 section.**

Task list to Upgrade to Unity Connection Shipping Version 10.x

Do the following tasks to upgrade an Unity Connection server:

1. If you are running the current version of Unity Connection on a physical server then you must replace it with a virtual server. See the Migrating a Physical Server to a Virtual Machine, page 5-1 section.

   If you are already running the current version on a virtual server, make sure it is compatible with the upgraded version. See the *Cisco Unity Connection 10.x Supported Platform List* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/supported_platforms/10xcucspl.html.

Note If you are performing an L2 upgrade, make sure that the Platform SOAP services are running on both the Unity Connection servers to successfully upgrade using Prime Collaboration Deployment. SOAP services can be enabled on both the servers using Cisco Unified Serviceability page. For more information on PCD, see the *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/pcdadmin/10_0_1/CUCM_BK_U9C58CB1_00_pcd-administration-guide-1001.html.

2. If you are upgrading during non business hours, run the following command on the standalone server or the publisher server to speed up the upgrade process:

   utils iothrottle disable

   If you are upgrading during a maintenance window, you can speed up the upgrade by disabling the throttling. This decreases the time required to complete the upgrade but affects Unity Connection performance.

⚠ **Caution** You cannot disable throttling during the upgrade process. If you want to disable the throttling process, you must first stop upgrade, disable throttle, and restart the Unity Connection server. Once the server is active again, begin the upgrade process.

3. (*Unity Connection 8.6 only*) Install the licenses on the existing Unity Connection 8.6 servers before you upgrade to Unity Connection 10.x server. While upgrade, the legacy license information is uploaded in Unity Connection database. For more information, see the Migrating Licenses from Unity Connection 8.6 and Earlier Releases, page 6-3 section.
4. (*Unity Connection 7.x only*) Unity Connection version 7.0(1) and 7.1(2) cannot be directly upgraded to Unity Connection 10.x and higher versions. If you are currently running versions earlier than Unity Connection 7.1(3), you first need to upgrade to an intermediate version of Unity Connection 7.1(3). For information on supported upgrades, see the "Supported Cisco Unified Communications Manager Upgrades" section of *Cisco Unified Communications Manager Software Compatibility Matrix* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.
5. Confirm if you require COP file for the upgrade process from Table 3-1 and download file from http://software.cisco.com/download/navigator.html?mdfid=280082558&i=rm.
6. Apply the COP file using the steps listed in the Applying COP file from a Network Location section
7. Follow the upgrade process on the standalone server:
   - (*RU upgrades only)* Upgrade the server following the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section. The server automatically switches to the new version after completing the upgrade.
   - (*L2 upgrades only*) Upgrade the server using the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section. Switch to the upgraded software to complete the upgrade process following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software, page 3-8 section.
8. Follow the upgrade process on the Unity Connection cluster:
   - (*RU upgrades only)* Upgrade the publisher server following the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section. The server automatically switches to the new version after completing the upgrade.

     Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section. The server automatically switches to the new version after completing the upgrade.
   - (*L2 upgrades only*) Upgrade the publisher server using the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section.

   ⚠ **Caution** In case of L2 upgrade of a cluster, do not restart or perform switch version on the publisher server before completing the upgrade on subscriber server otherwise cluster will not function properly.

Upgrade the subscriber server following the steps mentioned in the Upgrading the Unity Connection Server, page 3-7 section.

Switch to the upgraded software first on the publisher server and then on the subscriber server following the steps mentioned in the Switching to the Upgraded Version of Unity Connection Software, page 3-8 section.

9. Confirm that publisher server has **Primary** status and subscriber server has **Secondary** status.

Upgrading the Unity Connection Server

To Upgrade the Unity Connection Server

Step 1 Do any one of the following:

- Copy the ISO file to a folder on an FTP or SFTP server that the Unity Connection server can access.
- Insert the DVD with the ISO file of the Unity Connection server that you want install into the disk drive of the server.

Step 2 Sign in to Cisco Unified Operating System Administration.

Step 3 From the **Software Upgrades** menu, select **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the **Source** field, select any one of the following:

- **Remote Filesystem:** Select this option to upgrade from remoter server and follow this procedure.
- **DVD/CD**: Select this option to upgrade from disk drive and move to Step 10.

Step 5 In the **Directory** field, enter the path of the folder that contains the upgrade file.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the upgrade file is in the upgrade folder, you must enter /upgrade).

If the upgrade file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter the alias that will be used to sign in to the remote server.

Step 8 In the **User Password** field, enter the password that will be used to sign in to the remote server.

Step 9 In the **Transfer Protocol** field, select the applicable transfer protocol and select **Next**.

Step 10 Select the upgrade version that you want to install and select **Next**. The upgrade file is copied to the hard disk of the Unity Connection server. When the file is copied, a screen displaying the checksum value appears.

Step 11 Verify the checksum.

Step 12 On the next page, monitor the progress of the upgrade.

Caution If you loose your connection with the remote server or close your browser during this step, you may see the following warning when you try to view the Software Installation/Upgrade page again:

Warning: Another session is installing software, click Assume Control to take over the installation.

To continue monitoring the upgrade, select **Assume Control**.

Step 13 Select **Next**.

During the initial phase of upgrade, the **Installation Log** text box in Cisco Unified Operating System Administration is updated with the information on the progress of the upgrade. To confirm the completion of upgrade, open the console of the Unity Connection server and make sure that a message indicating the completion of upgrade appears on the screen along with the login prompt.

Step 14 To verify if the upgrade is successful, run the following CLI commands:

- **show cuc version**: Displays the version of Unity Connection server in both active and inactive partitions. The upgraded Unity Connection version is in the inactive partition.
- **utils system upgrade status**: Displays the status of the upgrade that you performed. This command should display the message for successful upgrade along with the upgraded version.

Switching to the Upgraded Version of Unity Connection Software

After completing the upgrade process, you need to manually switch over to the upgraded version of Unity Connection. For a single Unity Connection server, you can select either **manual switch version** or **automatic switch version**.

You can perform the switch version running the CLI command **utils system switch-version**. The system automatically reboots after the switch version.

If you choose not to automatically switch to the upgraded partition at the end of the upgrade, do the following procedure when you are ready to switch partitions.

To Switch to the Upgraded Version of Unity Connection Software

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the **Settings** menu, select **Version**.

Step 3 On the Version Settings page, select **Switch Versions**, to start the following activities:

- Unity Connection services are stopped.
- Data from the active partition is copied to the inactive partition. Note that the messages are stored in a common partition, therefore they are not copied.
- The Unity Connection server restarts and switches to the newer version.

Note You can check the status of the upgraded software run the CLI command **show cuc version**. The upgrade is complete when the inactive partition has the upgraded software and the active partition has the old software.

Applying COP file from a Network Location

To Apply a COP file from Network Location

Step 1 Copy the Cisco Option Package (.cop) file on an FTP or SFTP server that the server can access.

Step 2 Sign in to Cisco Unified Operating System Administration.

If you are upgrading the subscriber server in a Unity Connection cluster, type the following address to access Cisco Unified Operating System Administration:

http://<Unity Connection_servername>/cmplatform

Step 3 From the **Software Upgrades** menu, select **Install/Upgrade**.

Step 4 On the Software Installation/Upgrade page, in the **Source** field, select **Remote Filesystem**.

Step 5 In the **Directory** field, enter the path to the folder that contains the .cop file.

If the .cop file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the folder path. (For example, if the .cop file is in the cop folder, you must enter /cop).

If the .cop file is located on a Windows server, you must use the applicable syntax for an FTP or SFTP server such as:

- The path must begin with a forward slash (/) and contain forward slashes throughout instead of backward slashes (\).
- The path must start from the FTP or SFTP root folder on the server and must not include a Windows absolute path that starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter the alias that will be used to sign in to the remote server.

Step 8 In the **User Password** field, enter the password that will be used to sign in to the remote server.

Step 9 In the **Transfer Protocol** field, select the applicable transfer protocol and select **Next**.

Step 10 Select the software that you want to install, and select **Next**.

The .cop file is copied to the virtual hard disk on Unity Connection server. When the file is copied, a screen displays the checksum value.

Step 11 Verify the checksum and select **Next** to begin the installation.

During the upgrade, the value of the **Status** field is **Running**. When the upgrade process is complete, the value of the **Status** field changes to **Complete**.

Note

- All command-line interface sessions are terminated automatically.
- The Cisco Tomcat Service can take several minutes to restart automatically.

Step 12 Sign out from the Cisco Unified Operating System Administration application.

Step 13 Run the CLI command **utils service list** to confirm that the Cisco Tomcat service is in the **Running** state.

Rollback of Unity Connection

After upgrading the Unity Connection version, you can rollback to the software version that was running before the upgrade by switching to the software version on inactive partition.

Important Considerations for Rollback

1. Do not make any configuration changes during the rollback because the changes are lost after the rollback.
2. In an cluster setup, do not switch versions on both the first and second servers at the same time. Perform switch version on the second server only after you have switched versions on the first server.
3. Users and mailbox stores that were added after the upgrade will no longer exist after you rollback to the version on inactive partition. The new users and mailbox stores will be deleted.
4. All messages are preserved but for the users that were added after upgrade, their messages are orphaned as the users no longer exist after rollback. These messages are moved to the undeliverable messages folder.
5. If you moved mailboxes from one mailbox store to another after upgrading, those mailboxes will be moved back to the mailbox stores they were in before the upgrade.
6. A future delivery folder is created for users to mark messages for future delivery. If you revert to a version that supports future delivery but the future delivery folder has not been created for the user as yet, the messages in the future delivery folder for the new version are moved to the undeliverable messages folder.
7. (*Unity Connection 8.5 and earlier only*) If a user rollbacks to Unity Connection version 8.5 or earlier from a current version that is 8.6 and higher, then following limitations are faced:
   - No voice messages will be left after the rollback.
   - No administrator settings are preserved after the rollback.

Rollback Scenarios

You can revert a single Unity Connection server or a cluster to the version on inactive partition.

To rollback a Unity Connection cluster, you should rollback both the servers, first the publisher and then the subscriber. After the successful rollback of both the publisher and subscriber servers, reset the replication between the two servers running the following CLI commands:

a. Stop the replication on subscriber server with the CLI command **utils dbreplication stop**.
b. Stop the replication on publisher server with the CLI command **utils dbreplication stop**.
c. Reset the replication running the CLI command **utils dbreplication reset all** on the publisher server.

After the reset of replication between the two servers, check the cluster status running the CLI command **show cuc cluster status utils system restart** on both publisher and subscriber.

To Rollback a Unity Connection Server to the Version in the Inactive Partition

Step 1 Sign in to Cisco Unified Operating System Administration.

Step 2 From the **Settings** menu, select **Version** and the Version Settings window displays.

Step 3 Select the **Switch Versions** option. After you confirm that you want to restart the system, the system restarts that might take up to 15 minutes.

Step 4 Follow the given steps to confirm that the switch version is successful:

a. Sign in to Cisco Unified Operating System Administration.

b. In the **Settings** menu, select **Version**. The Version Settings window displays the product version.

c. Confirm that the active partition runs the correct version of Unity Connection server and all critical services are in the **Running** state.

d. Sign in to Cisco Unity Connection Administration and confirm that the configuration data exists.

CHAPTER 4

Configuring Cisco Unity Connection Cluster

The Cisco Unity Connection cluster deployment provides high availability voice messaging through the two servers that run the same versions of Unity Connection. The first server in the cluster is the publisher server and the second server is the subscriber server.

Task List for Configuring a Unity Connection Cluster

Do the following tasks to create a Unity Connection cluster:

1. Gather Unity Connection cluster requirements. For more information, see *System Requirements for Cisco Unity Connection Release 10.x* at www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
2. Install the publisher server. For more information, see the Installing the Publisher Server, page 1-12 section.
3. Install the subscriber server. For more information, see the Installing the Subscriber Server, page 1-15 section.
4. Configure the Cisco Unified Real-Time Monitoring Tool for both publisher and subscriber servers to send notifications for the following Unity Connection alerts:
   - **AutoFailbackFailed**
   - **AutoFailbackSucceeded**
   - **AutoFailoverFailed**
   - **AutoFailoverSucceeded**
   - **NoConnectionToPeer**
   - **SbrFailed**

   For instructions on setting up alert notification for Unity Connection alerts, see the “Cisco Unified Real-Time Monitoring Tool” section of the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for the required release, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
5. *(Optional)* Do the following tasks to customize the cluster settings on the publisher server:
   a. Sign in to Cisco Unity Connection Administration.
   b. Expand **System Settings > Advanced** and select **Cluster Configuration**.
   c. On the Cluster Configuration page, change the server status and select **Save**. For more information on changing the server status in a cluster, see **Help> This Page**.

Note Cluster configuration is not supported with Cisco Unified Communications Manager Business Edition 5000.

Administering a Unity Connection Cluster

You must check the Unity Connection cluster status to ensure that the cluster is correctly configured and working properly. It is also important to understand the different server status in a cluster and the effects of changing a server status in a cluster.

Checking the Cluster Status

You can check the Unity Connection cluster status either using web interface or Command Line Interface (CLI).

Steps to Check the Unity Connection Cluster Status from Web Interface

Step 1 Sign in to Cisco Unity Connection Serviceability of either publisher or subscriber server.

Step 2 Expand **Tools** and select **Cluster Management**.

Step 3 On the Cluster Management page, check the server status. For more information about server status, see the Server Status and its Functions in a Unity Connection Cluster, page 4-5 section.

Steps to Check Unity Connection Cluster Status from Command Line Interface (CLI)

Step 1 You can run the **show cuc cluster status** CLI command on the publisher server or subscriber server to check the cluster status.

Step 2 For more information about server status and its related functions, see the Server Status and its Functions in a Unity Connection Cluster, page 4-5 section.

Managing Messaging Ports in a Cluster

In a Unity Connection cluster, the servers share the same phone system integrations. Each server is responsible for handling a share of the incoming calls for the cluster (answering phone calls and taking messages).

Depending on the phone system integration, each voice messaging port is either assigned to a specific server or used by both servers. Table 4-1 describes the port assignments.

Table 4-1 Server Assignments and Usage of Voice Messaging Ports in a Unity Connection Cluster

Integration Type	Server Assignments and Usage of Voice Messaging Ports
Integration by Skinny Client Control Protocol (SCCP) with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express	• The phone system is set up with twice the number of SCCP voicemail port devices that are needed to handle the voice messaging traffic. (For example, if 16 voicemail port devices are needed to handle all voice messaging traffic, 32 voicemail port devices must be set up on the phone system.) • In Cisco Unity Connection Administration, the voice messaging ports are configured so that half the number of the ports set up on the phone system are assigned to each server in the cluster. (For example, each server in the cluster has 16 voice messaging ports.) • On the phone system, a line group, hunt list, and hunt group are configured to enable the subscriber server answer most of the incoming calls for the cluster. • If one of the servers stops functioning (for example, when it is shut down for maintenance), the remaining server assumes responsibility of handling all incoming calls for the cluster. • When the server that stopped functioning is able to resume its normal functions and is activated, it resumes the responsibility of handling its share of incoming calls for the cluster.
Integration through a SIP Trunk with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express	• In Cisco Unity Connection Administration, half the number of voice messaging ports that are needed to handle voice messaging traffic are assigned to each server in the cluster. (For example, if 16 voice messaging ports are needed to handle all voice messaging traffic for the cluster, each server in the cluster is assigned 8 voice messaging ports.) • On the phone system, a route group, route list, and route pattern are configured to distribute calls equally between both servers in the cluster. • If one of the servers stops functioning (for example, when it is shut down for maintenance), the remaining server assumes responsibility of handling all incoming calls for the cluster. • When the server that stopped functioning is able to resume its normal functions and is activated, it resumes responsibility of handling its share of incoming calls for the cluster.

Table 4-1 Server Assignments and Usage of Voice Messaging Ports in a Unity Connection Cluster (continued)

Integration Type	Server Assignments and Usage of Voice Messaging Ports
Integration through PIMG/TIMG units	• The number of ports set up on the phone system is the same as the number of voice messaging ports on each server in the cluster so that the servers share all the voice messaging ports. (For example, if the phone system is set up with 16 voice messaging ports, each server in the cluster must have the same 16 voice messaging ports.) • On the phone system, a hunt group is configured to distribute calls equally to both servers in the cluster. • The PIMG/TIMG units are configured to balance the voice messaging traffic between the servers. • If one of the servers stops functioning (for example, when it is shut down for maintenance), the remaining server assumes responsibility of handling all the incoming calls for the cluster. • When the server that stopped functioning is able to resume its normal functions and is activated, it resumes responsibility of handling its share of incoming calls for the cluster.
Other integrations that use SIP	• In Cisco Unity Connection Administration, half the number of voice messaging ports that are needed to handle voice messaging traffic are assigned to each server in the cluster. (For example, if 16 voice messaging ports are needed to handle all voice messaging traffic for the cluster, each server in the cluster has 8 voice messaging ports.) • On the phone system, a hunt group is configured to distribute calls equally to both servers in the cluster. • If one of the servers stops functioning (for example, when it is shut down for maintenance), the remaining server assumes responsibility of handling all incoming calls for the cluster. • When the server that stopped functioning is able to resume its normal functions, it resumes responsibility of handling its share of incoming calls for the cluster.

Stopping All Ports from Taking New Calls

Follow the steps in this section to stop all the ports on a server from taking any new calls. Calls in progress continue until the callers hang up.

Tip Use the Port Monitor page in the Real-Time Monitoring Tool (RTMT) to determine whether any port is currently handling calls for the server. For more information, see the Step a.

To Stop All Ports on a Unity Connection Server from Taking New Calls

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 Expand the **Tools** menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Port Manager, in the **Change Port Status** column, select **Stop Taking Calls** for the server.

Restarting All Ports to Take Calls

Follow the steps in this section to restart all the ports on a Unity Connection server to allow them take calls again after they were stopped.

To Restart All Ports on a Unity Connection Server to Take Calls

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 Expand the **Tools** menu, select **Cluster Management**.

Step 3 On the Cluster Management page, under Port Manager, in the **Change Port Status** column, select **Take Calls** for the server.

Server Status and its Functions in a Unity Connection Cluster

Each server in the cluster has a status that appears on the Cluster Management page of Cisco Unity Connection Serviceability. The status indicates the functions that the server is currently performing in the cluster, as described in Table 4-2.

Table 4-2 Server Status in a Unity Connection Cluster

Server Status	Responsibilities of the Sever in a Unity Connection Cluster
Primary	• Publishes the database and message store both of which are replicated to the other server in the cluster. • Receives replicated data from the other server. • Displays and accepts changes to the administrative interfaces, such as Unity Connection Administration and Cisco Unified Operating System Administration. This data is replicated to the other server in the cluster. • Answers phone calls and takes messages. • Sends message notifications and MWI requests. • Sends SMTP notifications and VPIM messages. • Synchronizes voice messages in Unity Connection and Exchange mailboxes if the unified messaging feature is configured. • Connects with the clients, such as email applications and the web tools available through Cisco PCA. **Note** A server with **Primary** status cannot be deactivated.
Secondary	• Receives replicated data from the server with **Primary** status. Data includes the database and message store. • Replicates data to the server with **Primary** status. • Displays and accepts changes to the administrative interfaces, such as Unity Connection Administration and Cisco Unified Operating System Administration. The data is replicated to the server with **Primary** status. • Answers phone calls and takes messages. • Connects with the clients, such as email applications and the web tools available through Cisco PCA. **Note** Only a server with **Secondary** status can be deactivated.
Deactivated	• Receives replicated data from the server with **Primary** status. Data includes the database and message store. • Does not display the administrative interfaces, such as Unity Connection Administration and Cisco Unified Operating System Administration. The data is replicated to the server with **Primary** status. • Does not answer phone calls or take messages. • Does not connect with the clients, such as email applications and the web tools available through Cisco PCA.
Not Functioning	• Does not receive replicated data from the server with **Primary** status. • Does not replicate data to the server with **Primary** status. • Does not display the administrative interfaces, such as Unity Connection Administration and Cisco Unified Operating System Administration. • Does not answer phone calls or take messages. **Note** A server with **Not Functioning** status is usually shut down.

Table 4-2 Server Status in a Unity Connection Cluster (continued)

Server Status	Responsibilities of the Sever in a Unity Connection Cluster
Starting	• Receives replicated database and message store from the server with **Primary** status. • Replicates data to the server with **Primary** status. • Does not answer phone calls or take messages. • Does not synchronize voice messages between Unity Connection and Exchange mailboxes (single inbox). **Note** This status lasts only a few minutes, after which the server takes the applicable status.
Replicating Data	• Sends and receives data from the cluster. • Does not answer phone calls or take messages for sometime. • Does not connect with clients, such as email applications and the web tools available through the Cisco PCA for sometime. **Note** This status lasts only a few minutes, after which the previous status resumes for the server.
Split Brain Recovery (*After detecting two servers with Primary status)*	• Updates the database and message store on the server that is determined to have **Primary** status. • Replicates data to the other server. • Does not answer phone calls or take messages for sometime. • Does not synchronize voice messages between Unity Connection and Exchange mailboxes if single inbox is turned on for sometime. • Does not connect with clients, such as email applications and the web tools available through the Cisco PCA for sometime. **Note** This status lasts only a few minutes, after which the previous status resumes for the server.

Changing Server Status in a Cluster and its Effects

The Unity Connection cluster status can be changed either automatically or manually.

You can manually change the status of servers in a cluster in the following ways:

- A server with **Secondary** status can be manually changed to **Primary** status. See the Manually Changing the Server Status from Secondary to Primary, page 4-7 section.
- A server with **Secondary** status can be manually changed to **Deactivated** status. See the Manually Activating a Server with Deactivated Status, page 4-8 section.
- A server with **Deactivated** status can be manually activated so that its status changes to **Primary** or **Secondary**, depending on the status of the other server. See the Manually Activating a Server with Deactivated Status, page 4-8 section.

Manually Changing the Server Status from Secondary to Primary

To Manually Change the Server Status from Secondary to Primary

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 From the **Tools** menu, select **Cluster Management**.

Step 3 On the Cluster Management page, from the **Server Manager** menu, in the **Change Server Status** column of the server with **Secondary** status, select **Make Primary**.

Step 4 When prompted to confirm the change in server status, select **OK**.

The **Server Status** column displays the changed status when the change is complete.

Note The server that originally had **Primary** status automatically changes to **Secondary** status.

Manually Changing from the Server Status from Secondary to Deactivated

To Manually Change the Server Status from Secondary to Deactivated

Step 1 Sign in to the Real-Time Monitoring Tool (RTMT).

Step 2 From the **Cisco Unity Connection** menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

Step 3 In the **Node** field, select the server with **Secondary** status.

Step 4 In the right pane, select **Start Polling**. Note whether any voice messaging ports are currently handling calls for the server.

Step 5 Sign in to Cisco Unity Connection Serviceability.

Step 6 From the **Tools** menu, select **Cluster Management**.

Step 7 If no voice messaging ports are currently handling calls for the server, skip to Step 8.

If there are voice messaging ports that are currently handling calls for the server, on the Cluster Management page, in the **Change Port Status** column, select **Stop Taking Calls** for the server and then wait until RTMT shows that all ports for the server are idle.

Step 8 On the Cluster Management page, from the **Server Manager** menu, in the **Change Server Status** column for the server with **Secondary** status, select **Deactivate**.

Caution Deactivating a server terminates all the calls that the ports for the server are handling.

Step 9 When prompted to confirm the change in the server status, select **OK**.

The **Server Status** column displays the changed status when the change is complete.

Manually Activating a Server with Deactivated Status

To Manually Activate a Server with Deactivated Status

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 From the **Tools** menu, select **Cluster Management**.

Step 3 On the Cluster Management page, in the **Server Manager** menu, in the **Change Server Status** column for the server with **Deactivated** status, select **Activate**.

Step 4 When prompted to confirm the change in the server status, select **OK**.

The **Server Status** column displays the changed status when the change is complete.

Effect on Calls in Progress When Server Status Changes in a Unity Connection Cluster

When the status of a Unity Connection server changes, the effect on calls in progress depend upon the final status of the server that is handling a call and on the condition of the network. The following table describes the effects:

Table 4-3 Effect on Calls in Progress When Server Status Changes in a Unity Connection Cluster

Status Change	Effects
Primary to Secondary	When the status change is initiated manually, calls in progress are not affected. When the status change is automatic, effect on calls in progress depend on the critical service that stopped.
Secondary to Primary	When the status change is initiated manually, calls in progress are not affected. When the status change is automatic, effect on calls in progress depend upon the critical service that stopped.
Secondary to Deactivated	Calls in progress are dropped. To prevent dropped calls, on the Cluster Management page in Cisco Unity Connection Serviceability, select **Stop Taking Calls** for the server and wait until all the calls get ended and deactivate the server.
Primary or Secondary to Replicating Data	Calls in progress are not affected.
Primary or Secondary to Split Brain Recovery	Calls in progress are not affected.

If network connections are lost, then calls in progress may be dropped depending upon the nature of the network problem.

Effect on Unity Connection Web Applications When the Server Status Changes

The functioning of the following web applications is not affected when the server status changes:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unity Connection web tools accessed through the Cisco PCA—the Messaging Assistant, Messaging Inbox, and Personal Call Transfer Rules web tools
- Cisco Web Inbox
- Representational state transfer (REST) API clients

Effect of Stopping a Critical Service on a Unity Connection Cluster

Critical services are necessary for the normal functioning of the Unity Connection system. The effects of stopping a critical service depend upon the server and its status described in the following table:

Table 4-4 Effects of Stopping a Critical Service on a Unity Connection Cluster

Server	Effects
Publisher	• When the server has **Primary** status, stopping a critical service in Cisco Unity Connection Serviceability causes the server status to change to **Secondary** and degrades the ability of the server to function normally. The status of the subscriber server changes to **Primary** if it does not have the Disabled or Not Functioning status. • When the server has **Secondary** status, stopping a critical service in Cisco Unity Connection Serviceability degrades the ability of the server to function normally. The status of the servers does not change.
Subscriber	When the server has **Primary** status, stopping a critical service in Cisco Unity Connection Serviceability degrades the ability of the server to function normally. The status of the servers does not change.

Shutting Down a Server in a Cluster

When a Unity Connection server has **Primary** or **Secondary** status, it is handles voice messaging traffic and cluster data replication. We do not recommend you to shutdown both the servers in a cluster at the same time to avoid abrupt termination of the calls and replication that are in progress.

Consider the following points when you want to shutdown a server in a Unity Connection cluster:

- Shutdown the server during non business hours when voice messaging traffic is low.
- Change the server status from **Primary** or **Secondary** to **Deactivated** before shutting down.

To Shutdown a Server in a Unity Connection Cluster

Step 1 On the server that will not be shut down, sign in to Cisco Unity Connection Serviceability.

Step 2 From the **Tools** menu, select **Cluster Management**.

Step 3 On the Cluster Management page, locate the server that you want to shut down.

Step 4 If the server that you want to shut down has **Secondary** status, skip to Step 5.

If the server that you want to shut down has **Primary** status, change the status:

a. In the **Change Server Status** column for the server with **Secondary** status, select **Make Primary**.

b. When prompted to confirm the change in the server status, select **OK**.

c. Confirm that the **Server Status** column indicates that the server has **Primary** status now and that the server you want to shut down has **Secondary** status.

Step 5 On the server with **Secondary** status (the one you want to shut down), change the status:

a. Sign in to the Real-Time Monitoring Tool (RTMT).

b. From the **Cisco Unity Connection** menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.

c. In the **Node** field, select the server with Secondary status.

d. In the right pane, select **Start Polling**.

e. Note whether any voice messaging ports are currently handling calls for the server.

f. If no voice messaging ports are currently handling calls for the server, skip to Step5g..

If there are voice messaging ports that are currently handling calls for the server, on the Cluster Management page, in the **Change Port Status** column, select **Stop Taking Calls** for the server and then wait until RTMT shows that all ports for the server are idle.

g. On the Cluster Management page, from the **Server Manager** menu, in the **Change Server Status** column for the server with **Secondary** status, select **Deactivate**.

⚠ **Caution** Deactivating a server will terminate all calls that the ports for the server are handling.

h. When prompted to confirm the change in the server status, select **OK**.

i. Confirm that the **Server Status** column indicates that the server now has **Deactivated** status.

Step 6 Shut down the server that you deactivated:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand **Tools** and select **Cluster Management**.

c. Make sure that the **Server Status** column shows **Not Functioning** status for the server that you shutdown.

Replacing Servers in a Cluster

Follow the steps in the given sections to replace publisher or subscriber server in a cluster:

- To replace the publisher server, see the Replacing a Publisher Server, page 5-2 section.
- To replace the subscriber server, see the Replacing a Subscriber Server, page 5-3 section.

Understanding Cluster in Detail

To understand the Unity Connection cluster in detail, follow the given sections:

- How a Unity Connection Cluster Works, page 4-12
- Effects of Split Brain Condition in a Unity Connection Cluster, page 4-13

How a Unity Connection Cluster Works

The Unity Connection cluster feature provides high availability voice messaging through two Unity Connection servers that are configured in a cluster.

The Unity Connection cluster behavior when both the servers are active:

- The cluster can be assigned a DNS name that is shared by the Unity Connection servers.
- Clients, such as email applications and the web tools available through the Cisco Personal Communications Assistant (PCA) can connect to either of the Unity Connection server.
- Phone systems can send calls to either of the Unity Connection server.
- Incoming phone traffic load is balanced between the Unity Connection servers by the phone system, PIMG/TIMG units, or other gateways that are required for the phone system integration.

Each server in a cluster is responsible for handling a share of the incoming calls for the cluster (answering phone calls and taking messages). The server with **Primary** status is responsible for the following functions:

- Homing and publishing the database and message store that are replicated to the other server.
- Sending message notifications and MWI requests (the **Connection Notifier** service is activated).
- Sending SMTP notifications and VPIM messages (the **Connection Message Transfer Agent** service is activated).
- Synchronizing voice messages between Unity Connection and Exchange mailboxes, if the unified messaging feature is configured (the **Unity Connection Mailbox Sync** service is activated).

When one of the servers stops functioning (for example, when it is shutdown for maintenance), the remaining server resumes the responsibility of handling all the incoming calls for the cluster. The database and message store are replicated to the other server when its functionality is restored.

When the server that stopped functioning is able to resume its normal functions and is activated, it resumes responsibility of handling its share of incoming calls for the cluster.

To monitor the server status, the **Connection Server Role Manager** service runs in Cisco Unity Connection Serviceability on both the servers. This service performs the following functions:

- Starts the applicable services on each server, depending on server status.
- Determines whether critical processes (such as voice message processing, database replication, voice message synchronization with Exchange, and message store replication) are functioning normally.
- Initiates changes to server status when the server with **Primary** status is not functioning or when critical services are not running.

Note the following limitations when the publisher server is not functioning:

- If the Unity Connection cluster is integrated with an LDAP directory, directory synchronization does not occur, although authentication continues to work when only the subscriber server is functioning. When the publisher server is resumes functioning, directory synchronization also resumes.
- If a digital or HTTPS network includes the Unity Connection cluster, directory updates do not occur, although messages continue to be sent to and from the cluster when only the subscriber server is functioning. When the publisher server is functioning again, directory updates resume.

The **Connection Server Role Manager** service sends a keep-alive events between the publisher and subscriber servers to confirm that the servers are functioning and connected. If one of the servers stops functioning or the connection between the servers is lost, the **Connection Server Role Manager** service waits for the keep-alive events and may require 30 to 60 seconds to detect that the other server is not available. While the **Connection Server Role Manager** service is waiting for the keep-alive events, users signing in to the server with Secondary status will not be able to access their mailbox or send messages, because the **Connection Server Role Manager** service has not yet detected that the server with Primary status (which has the active message store) is unavailable. In this situation, callers who attempt to leave a message may hear dead air or may not hear the recording beep.

Note It is recommended to import and delete the LDAP users from the publisher node only.

Effects of Split Brain Condition in a Unity Connection Cluster

When both the servers in a Unity Connection cluster have **Primary** status at the same time (for example, when the servers have lost their connection with each other), both servers handle the incoming calls (answer phone calls and take messages), send message notifications, send MWI requests, accept changes to the administrative interfaces (such as Unity Connection Administration), and synchronize voice messages in Unity Connection and Exchange mailboxes if single inbox is turned on. However, the servers do not replicate the database and message store to each other and do not receive replicated data from each other.

When the connection between the servers is restored, the status of the servers temporarily changes to **Split Brain Recovery** while the data is replicated between the servers and MWI settings are coordinated. During the time when the server status is **Split Brain Recovery**, the **Connection Message Transfer Agent** service and the **Connection Notifier** service (in Cisco Unity Connection Serviceability) are stopped on both servers, so Unity Connection does not deliver any messages and does not send any message notifications. The **Connection Mailbox Sync** service is also stopped, so Unity Connection does not synchronize voice messages with Exchange (single inbox). The message stores are also briefly dismounted, so that Unity Connection tells users who are trying to retrieve their messages at this point that their mailboxes are temporarily unavailable.

When the recovery process is complete, the **Connection Message Transfer Agent** service and the Connection Notifier service are started on the publisher server. Delivery of the messages that arrived while during the recovery process may take additional time, depending on the number of messages to be delivered. The **Connection Message Transfer Agent** service and the Connection Notifier service are started on the subscriber server. Finally, the publisher server has Primary status and the subscriber server has **Secondary** status. At this point, the **Connection Mailbox Sync** service is started on the server with **Primary** status, so that Unity Connection can resume synchronizing voice messages with Exchange if single inbox is turned on.

CHAPTER 5

Maintaining Cisco Unity Connection Server

This chapter explains following procedures that can be performed on a Cisco Unity Connection server

- Migrating a Physical Server to a Virtual Machine, page 5-1
- Migrating from Cisco Unity 4.x and Later to Unity Connection 7.x and Later, page 5-4
- Replacing the Non-Functional Server, page 5-5
- Changing the IP Address or Hostname of a Unity Connection Server, page 5-6
- Adding or Removing Unity Connection Languages, page 5-9

Migrating a Physical Server to a Virtual Machine

Follow the given tasks to migrate from physical server to a virtual machine:

- Backup the software component on the physical server. For more information, see the "Backing Up and Restoring Cisco Unity Connection Components" chapter.
- Download and deploy the OVA template to create a new virtual machine. For more information, see the Creating a Virtual Machine, page 1-3 section.
- Migrating the Unity Connection server on the virtual machine.
  - To replace the publisher server, see the Replacing a Publisher Server, page 5-2 section.
  - To replace the subscriber server, see the Replacing a Subscriber Server, page 5-3 section.
- If Unity Connection is installed as a standalone server, restore the software component from the physical server to the virtual machine for which you have taken the back up. For more information, see the To Restore the Software Components on Unity Connection, page 2-6 section.
- (*Optional)* Install new languages on the replaced server if required or remove the existing languages already installed on the server. For more information, see the Adding or Removing Unity Connection Languages, page 5-9 section.

Note If you are deploying Unity Connection networking (Intersite, Intrasite, or HTTPS), see the *Networking Guide for Cisco Unity Connection, Release 10.x,* before replacing the Unity Connection server, available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/networking/guide/10xcucnetx.html.

Replacing a Publisher Server

While you are upgrading the publisher server in a Unity Connection cluster, the subscriber server continues to provide services to the users and callers.

Note In case of a standalone server, replace the server during off-peak hours to avoid call-processing interruptions and impact to services.

To Replace a Publisher Server

Step 1 Manually change the status of subscriber server to **Primary**:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand **Tools** and select **Cluster Management**.

c. On the Cluster Management page, from the **Server Manager** menu, locate the subscriber server and check the following:

- If the subscriber server status is **Primary**, skip the remaining steps in this procedure.
- If the subscriber server status is **Secondary**, select **Make Primary**.
- If the subscriber has **Deactivated** status, change the status to **Secondary** and then select **Activate**. When prompted to confirm changing the server status, select **OK**. After successful activation of the subscriber server, change the status to **Primary** selecting **Make Primary** option.

Step 2 Manually change the status of publisher server to **Deactivated**:

a. Sign in to the Real-Time Monitoring Tool and select **Port Monitor.**

b. In the **Node** field, select the publisher server and then select **Start Polling**. Note whether any voice messaging ports are currently handling calls for the server.

c. Return to the Cluster Management page of Cisco Unity Connection Serviceability and do any one of th following:

- If no voice messaging ports are currently handling calls for the publisher server, move to the next Step 3.
- If there are voice messaging ports that are currently handling calls for the publisher server, on the Cluster Management page, in the **Port Manager** column, select **Stop Taking Calls** for the publisher server and then wait until RTMT shows that all the ports for the publisher server are idle.

d. From the **Server Manager** menu, in the **Change Server Status** column for the publisher server, select **Deactivate** and then select **OK.**

Step 3 Install the replacement publisher server, see Installing the Publisher Server, page 1-12 section.

a. Shut down the publisher server using the CLI command **utils system shutdown**. On the Cluster Management page of the subscriber server, the publisher has **Not Functioning** status.

b. Install the virtual machine. The following settings on the virtual machine must be same as that on the physical server, otherwise the transfer of data from the physical server to the virtual machine will fail:

- Hostname of the server
- IP address of the server

- Time zone
- NTP server
- DHCP settings
- Primary DNS settings
- SMTP hostname
- X.509 Certificate information (Organization, Unit, Location, State, and Country).

Step 4 Configure the cluster on the replaced publisher server:

a. Sign in to Cisco Unity Connection Administration on the publisher server.

b. Expand **System Settings** and select **Cluster**.

c. On the Find and List Servers page, select **Add New**.

d. On the New Server Configuration page, in the **Hostname/IP Address** field, enter the hostname or IP address of the subscriber server. Enter the description and select **Save**.

Step 5 If Unity Connection is installed as a cluster, you can restore the publisher using the subscriber data.

a. Run the **utils cuc cluster renegotiate** CLI command on the subscriber server. The publisher automatically restarts after running this command.

b. Run the **show cuc cluster status** CLI command on the subscriber server to confirm that the new Unity Connection cluster is configured correctly.

Replacing a Subscriber Server

While you are upgrading the subscriber server in a Unity Connection cluster, the publisher server continues to provide services to users and callers.

To Replace a Subscriber Server

Step 1 Manually change the status of publisher server to **Primary**:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand **Tools** and select **Cluster Management**.

c. On the Cluster Management page, from the **Server Manager** menu, locate the publisher server and check the following:

- If the publisher server status is **Primary**, skip the remaining steps in this procedure.
- If the publisher server status is **Secondary**, change the status by selecting **Make Primary**.
- If the publisher has **Deactivated** status, change the status to **Secondary** and select **Activate**. A prompt appears to confirm the changing of the server status, select **OK**. After successful activation of the publisher server, change the status to **Primary** by selecting **Make Primary** option.

Step 2 Manually change the status of subscriber server to **Deactivated**:

a. Sign in to the Real-Time Monitoring Tool, expand <Unity Connection> option and select **Port Monitor**.

b. In the **Node** field, select the subscriber server and select **Start Polling**. Note whether any voice messaging ports are currently handling calls for the server.

c. Return to the Cluster Management page of Cisco Unity Connection Serviceability.

- If no voice messaging ports are currently handling calls for the server, skip to the next step.
- If there are voice messaging ports that are currently handling calls for the subscriber server, on the Cluster Management page, in the **Change Port Status** column, select **Stop Taking Calls** for the subscriber server and then wait until RTMT shows that all ports for the server are idle.

d. From the **Server Manager** menu, in the **Change Server Status** column for the subscriber server, select **Deactivate** and select **OK**.

Step 3 Make sure that the hostname or IP address of the subscriber server is configured correctly on the publisher server as mentioned in Step 4 of replacing a publisher server.

Step 4 Install the replaced subscriber server, see Installing the Subscriber Server, page 1-15 section.

a. Shut down the subscriber server using the CLI command **utils system shutdown**. On the Cluster Management page of the publisher server, the subscriber has **Not Functioning** status.

b. Reinstall the Unity Connection server. You must specify the same security password of the subscriber server that you are replacing and it should also match the security password for the publisher server. Otherwise, the Unity Connection cluster will not function. If you do not know the security password, you can change it on the publisher server before you install the subscriber server using the CLI command **set password user**.

Step 5 Check the cluster status by running the **show cuc cluster status** CLI command on the subscriber server.

Migrating from Cisco Unity 4.x and Later to Unity Connection 7.x and Later

To Migrate from Cisco Unity 4.x and Later to Unity Connection 7.x and Later

Step 1 If you are running the current version of Cisco Unity on a physical server then you must replace it with a virtual machine. For more information, see the Migrating a Physical Server to a Virtual Machine, page 5-1 section.

However, if you are already running the current version on a virtual machine, make sure it is compatible with the upgraded version. See the *Cisco Unity Connection 10.x Supported Platform List* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/supported_platforms/10xcucspl.html.

Step 2 Migrate the Cisco Unity licenses to a virtual machine. To migrate the licenses, a user sends a license request to the Cisco licensing support. The content for the requested license file is analyzed and an appropriate license file is sent back to the user, which is further installed on the Unity Connection server.

Step 3 Download the following tools:

- The Cisco Unity Disaster Recovery tools, available at http://www.ciscounitytools.com/Applications/Unity/DIRT/DIRT.html.
- Consolidated Object Backup and Restore Application Suite (COBRAS), available at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Step 4 If you want to use the Migration Export tool and if you do not have a secure shell (SSH) server application installed on a server that is accessible to the Cisco Unity server, then install an SSH server application. The migration tool imports Cisco Unity data into Unity Connection 10.x that uses SSH to access the exported user data and messages.

Step 5 (*Optional*) Use the Migration Export tool to export Cisco Unity data and messages. The data exported through the tool is required only if COBRAS fails for some reason.

Step 6 If you have a secure shell (SSH) server application installed on a server that is accessible to the Cisco Unity server, export the data to the SSH server. If you do not have an SSH server, you can export data to any network location. You can set up an SSH server later if necessary.

Step 7 Use COBRAS to export Cisco Unity data and, optionally, messages. For more information, see **Help** for the tool at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Step 8 Install and configure Unity Connection 10.x. For more information, see Installing Cisco Unity Connection, page 1-1 chapter.

Step 9 Restore Cisco Unity data on the Unity Connection server using COBRAS Import tool.

Replacing the Non-Functional Server

Table 5-1 Replacing the Non-Functional Server

Tasks	Procedure
If Unity Connection is installed as standalone.	• Recreate the virtual machine. For more information, see the Creating a Virtual Machine, page 1-3 section. • Restore the software. For more information, see the To Restore the Software Components on Unity Connection, page 2-6 section.
If Unity Connection is installed as a cluster and publisher is not functioning.	• Recreate the virtual machine. For more information, see the Creating a Virtual Machine, page 1-3 section. • Replace the Publisher server, see the Replacing a Publisher Server, page 5-2 section.

Tasks	Procedure
If Unity Connection is installed as a cluster and subscriber is not functioning.	Install the subscriber server, see the Installing the Subscriber Server, page 1-15 section.
If both the servers are not functioning in a cluster.	• Replace the publisher server, see Installing the Publisher Server, page 1-12 section. • Restore the software components on the physical machine. For more information, see the To Restore the Software Components on Unity Connection, page 2-6 section. • Configure cluster on the publisher sever: – Replace the subscriber server, see the Installing the Subscriber Server, page 1-15 section. – Check the cluster status using CLI command **show cuc cluster status**. – Synchronize MWIs on each phone system.

Changing the IP Address or Hostname of a Unity Connection Server

Before changing the IP address of a standalone Unity Connection server or a cluster, you need to determine whether the server is defined by hostname or IP address.

Note You can also use Cisco Prime Collaboration Deployment for readdressing. For more information on Cisco PCD, see http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.

Determine Whether Unity Connection is Defined by Hostname or IP Address

To Determine Whether Unity Connection is Defined by Hostname or IP Address

Step 1 Sign in to Cisco Unity Connection Administration of the server of which the IP address needs to be changed.

Step 2 Expand **System Settings** and select **Cluster.**

Note You need to select **Cluster** even if you want to change the IP address or hostname of a standalone server.

Step 3 Select **Find** to locate the server of which you need to change the IP address or hostname:

- If the value of the Hostname/IP Address column is a hostname, the server is defined by a hostname.

- If the value of the Hostname/IP Address column is an IP address, the server is defined by an IP address.

Important Considerations before Changing the Hostname or IP Address of a Unity Connection Server

1. When you change the IP address or hostname of the Unity Connection server, make sure to apply the same changes on all the associated components that refer the Unity Connection server by IP address or hostname:
2. Bookmarks on client computers to the following web applications:
   - Web applications, such as Cisco Personal Communications Assistant and Cisco Unity Connection Administration.
   - Cisco Fax Server
   - Cisco Unified Application Environment
   - Cisco Unified Mobile Advantage
   - Cisco Unified Presence
   - Cisco Unified Personal Communicator
   - Cisco Unity Connection ViewMail for Microsoft Outlook
   - IMAP email clients that access Unity Connection
   - Phone systems and related components, including Cisco EGW 2200, Cisco ISR voice gateway, Cisco SIP Proxy Server, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and PIMG/TIMG units.
   - RSS readers
   - SMTP smart host
   - Voice messaging systems with which Unity Connection is integrated via VPIM, such as Cisco Unity and Cisco Unity Express.

Caution If associated components reference the Unity Connection server by IP address and if you do not change the IP address as applicable, the components will no longer be able to access Unity Connection.

3. You can change the IP address and hostname of a Unity Connection server or cluster following the steps mentioned in the Changing the IP Address or Hostname of a Unity Connection Server or Cluster, page 5-8 section.

Caution Do not change the IP address or hostname of a Unity Connection server during business hours.

4. (*Only in case of changing IP address of a Unity Connection server*) If the Unity Connection server is configured to get an IP address from a DHCP server, you cannot manually change the IP address of the server. Instead, you must do one of the following:

- Change DHCP/DNS settings from Cisco Unified Operating System Administration> **Settings** and select the applicable option from **IP**, and restart Unity Connection by running the CLI command **utils system restart**.
- Disable DHCP on Unity Connection by running the CLI command **set network dhcp** and then manually change the IP address by doing the procedure given below.

Note To change the IP address or hostname of a Unity Connection cluster, follow the steps mentioned in the "Changing the IP Address or Hostname of a Unity Connection Server" section first on the publisher server and then on the subscriber server.

Changing the IP Address or Hostname of a Unity Connection Server or Cluster

Do the following steps to change the IP address or Hostname of a standalone server or a cluster defined by hostname. In case of a cluster, follow the steps first on the publisher server and then on the subscriber server.

To Change the IP Address of a Standalone or a Cluster Server

Step 1 Sign in to the standalone server or the publisher server using Real-Time Monitoring Tool. Expand **Tools> Alert** and select **Alert Central**. In the **Systems** tab, make sure the **ServerDown** is black. If **ServerDown** is red, then resolve all the problems and change it to black. Repeat the same step for the subscriber server (in case of a cluster).

Step 2 Check the server status:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand **Tools** and select **Cluster Management**.

c. On the Cluster Management page, check whether server status is **Primary** or **Secondary**. If there is any other status value then resolve the problem.

Step 3 Check the network connectivity and DNS server configuration by running the **utils diagnose module validate_network** CLI command**.**

Step 4 Backup the database using Disaster Recovery System. See the"Backing Up and Restoring Cisco Unity Connection Components" chapter.

Step 5 If intrasite, HTTPS, and SRSV networking is configured, remove the server from the Unity Connection site. For instructions, see the *Networking Guide for Cisco Unity Connection, Release 10.x*, available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/networking/guide/10xcucnetx.html.

Caution Re-adding a server to a Unity Connection site can be a time consuming process.

Step 6 On a DNS server, change the DNS record of the Unity Connection server to the new IP address. Update both the forward (A) and reverse (PTR) records.

Step 7 On the standalone or publisher server, change the IP address, Hostname, and default gateway (if applicable):

a. Sign in to Cisco Unified Operating System Administration.

b. From the **Settings** menu, select **IP** > **Ethernet**.

c. Specify an alternate hostname for the server by running the **set web-security** CLI command. In the **Hostname**, change the hostname of the server.

Note

- Enter a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA).
- (*In case of SSL certificates created and installed on renamed server)* Upload the root certificate and the server certificate to the standalone or publisher server. Follow the steps as mentioned in *Security Guide for Cisco Unity Connection Release 10.x,* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx/10xcucsecix.html.

d. In the **Port Information**, change the value of the **IP Address** and **Subnet Mask** field (if applicable).

e. If you are moving the server to a different subnet that requires a new default gateway address, change the value of the **Default Gateway** field in the **Gateway Information**.

f. Select **Save**.

g. Hard reboot the server.

Note In case of a standalone Unity Connection server, you need to do a hard reboot to reflect the changes in IP address or hostname of the server.

Step 8 Sign in to Real-Time Monitoring Tool and confirm that the server is available and running.

This completes the process of changing the IP address of the standalone server.

Step 9 For the cluster, repeat Step 1 to Step 8 on subscriber server also.

This completes the process of changing the IP address of a cluster.

Adding or Removing Unity Connection Languages

After installing a new server or on an existing server, you may need to add some new language(s) and remove some already installed languages depending on the user requirement.

Note Languages are not licensed and Unity Connection 10.x does not enforce a limit on the number of languages you can install and use. However, the more languages you install, the less hard disk space is available for storing voice messages.

Task List for Adding Languages to a Standalone Unity Connection Server

Do the following tasks to download and install languages in addition to English (United States):

1. Download the Unity Connection languages that you want to install and do the following steps:

a. Sign in as a registered user on the following Cisco.com link: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875240.

b. Expand Unified Communications Applications > Voicemail and Unified Messaging > Cisco Unity Connection, and select the applicable Unity Connection version.

c. On the Select a Software Type page, select **Cisco Unity Connection Locale Installer**.

d. On the Select a Release page, select the applicable Unity Connection version. The download links for the languages appear on the right side of the page.

e. Select the name of a file to download. On the Download Image page, note down the MD5 value and follow the on screen prompts to complete the download.

Note Make sure that the MD5 checksum matches the checksum that is listed on Cisco.com. If the values do not match, the downloaded file is damaged. Do not attempt to use a damaged file to install software as the results will be unpredictable. If the MD5 values do not match, download the file again until the value for the downloaded file matches the value listed on Cisco.com.

2. (*Unity Connection cluster only*) Make sure that the subscriber server status is **Primary** and the publisher server status is **Secondary** in order to install the Unity Connection languages. Follow the given steps:

   a. Sign in to Cisco Unity Connection Serviceability.

   b. Expand Tools and select **Cluster Management**.

   c. For subscriber server, select **Make Primary**.

3. On the standalone or publisher server, install the Unity Connection languages that you downloaded. Do any one of the following:

- Installing Unity Connection Language Files from a Disk, page 5-11
- Installing Unity Connection Language Files from Network Location or Remote Server, page 5-11

4. *If you are using additional languages because you want the Cisco Personal Communications Assistant to be localized:* Download and install the corresponding Unity Connection locales on the publisher server.

5. (*Unity Connection cluster only*) Change the publisher server status to **Primary** and follow the same steps on subscriber server to install the same Unity Connection languages that were installed on publisher server.

Installing Unity Connection Language Files

You can install language files on the Unity Connection server either through CD/DVD or by accessing the files through a remote source. See the following sections:

- Installing Unity Connection Language Files from a Disk, page 5-11
- Installing Unity Connection Language Files from Network Location or Remote Server, page 5-11

Installing Unity Connection Language Files from a Disk

To Install Unity Connection Language Files from a Disk

Step 1 Stop the **Connection Conversation Manager** and **Connection Mixer** services:

a. Sign in to Cisco Unity Connection Serviceability. Expand the **Tools** menu and select **Service Management**.

b. From the **Critical Services** menu, in the **Connection Conversation Manager** row, select **Stop**.

c. Wait for the service to stop.

d. From the **Critical Services** menu, in the **Connection Mixer** row, select **Stop**.

e. Wait for the service to stop.

Step 2 Insert the languages disk in the disk drive.

Step 3 Sign in to Cisco Unified Operating System Administration.

Step 4 From the **Software Upgrades** menu, select **Install/Upgrade**. The **Software Installation/Upgrade** window appears.

Step 5 In the **Source** list, select **DVD/CD**.

Step 6 In the **Directory** field, enter the path of the folder that contains the language file.

If the language file is in the root folder or if you created an ISO image DVD, enter a slash (/) in the **Directory** field.

Step 7 To continue the installation of language files, select **Next**.

Step 8 Select the language that you want to install, and select **Next**.

Step 9 Monitor the progress of the download.

Step 10 *If you want to install another language:* Select **Install Another**, and repeat all the steps.

If you are finished with installing languages: Restart the services:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand the **Tools** menu and select **Service Management**.

c. In the **Critical Services** menu, in the **Connection Conversation Manager** row, select **Start**.

d. Wait for the service to start.

e. In the **Critical Services** menu, in the **Connection Mixer** row, select **Start**.

f. Wait for the service to start.

Note You need to restart Cisco Tomcat service after you have installed language file from a disk.

Installing Unity Connection Language Files from Network Location or Remote Server

In this procedure, do not use the web browser controls (for example, Refresh/Reload) while accessing Cisco Unified Operating System Administration. However, you can use the navigation controls in the administration interface.

To Install Unity Connection Language Files from a Network Location or from a Remote Server

Step 1 Stop the **Connection Conversation Manager** and **Connection Mixer** services:

a. Sign in to Cisco Unity Connection Serviceability. Expand **Tools** menu and select **Service Management**.

b. In **Critical Services,** for the **Connection Conversation Manager** row, select **Stop**.

c. Wait for the service to stop.

d. In the **Critical Services** menu, in the **Connection Mixer** row, select **Stop**.

e. Wait for the service to stop.

Step 2 Sign in to Cisco Unified Operating System Administration.

Step 3 From the **Software Upgrades** menu, select **Install/Upgrade**. The **Software Installation/Upgrade** window appears.

Step 4 In the **Source** list, select **Remote Filesystem**.

Step 5 In the **Directory** field, enter the path of the folder that contains the language file on the remote system.

If the language file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the folder path. (For example, if the language file is in the languages folder, you must enter **/languages**.)

If the language file is located on a Windows server, make sure that you are connecting to an FTP or SFTP server, and use the appropriate syntax:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root folder on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 6 In the **Server** field, enter the server name or IP address.

Step 7 In the **User Name** field, enter your user name on the remote server.

Step 8 In the **User Password** field, enter your password on the remote server.

Step 9 In the **Transfer Protocol** list, select the applicable option.

Step 10 Select **Next**.

Step 11 Select the language that you want to install, and select **Next**.

Step 12 Monitor the progress of the download.

Note If you loose your connection with the server or close your browser during the installation process, you may see the following message when you try to access the Software Upgrades menu again:

Warning: Another session is installing software, click Assume Control to take over the installation.

If you are sure you want to take over the session, select **Assume Control**.

Step 13 *If you want to install another language,*: Select **Install Another**, and repeat all the above steps.

Step 14 *If you are finished with installing languages:* Restart the services:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand **Tools** menu and select **Service Management**.

c. In the **Critical Services** menu, in the **Connection Conversation Manager** row, select **Start**. Wait for the service to start.

d. In the **Critical Services** menu, in the **Connection Mixer** row, select **Start**. Wait for the service to start.

Note You need to restart Cisco Tomcat service after you have installed language file from a disk.

Removing Unity Connection Language Files

To Remove a Unity Connection Language File

Step 1 Sign in to the command line interface as a platform administrator.

Note Make sure to stop **Connection Conversation Manager** and **Connection Mixer** services before uninstalling the languages.

Step 2 Run the **show cuc locales** CLI command to display a list of installed language files.

Step 3 In the command results, find the language that you want to remove, and note the value of the **Locale** column for the language.

Step 4 Run the **delete cuc locale <code>** CLI command to remove the language, where <code> is the value of the Locale column that you get in Step 3.

When the command completes, the following information appears:

```
<code> uninstalled
```

CHAPTER 6

Managing Licenses

Cisco Unity Connection licenses are required to use various features supported with the product. To use various Unity Connection features, corresponding licenses must be installed on Prime License Manager (PLM) and Unity Connection must synchronize with the PLM server to obtain the desired license status.

Installing Licenses on the PLM server

Follow the given two steps to configure the Unity Connection licenses:

1. Install license on the PLM server. For more information, see the “New License Planning and Fulfillment” section in “Operation” chapter of *Cisco Prime License Manager User Guide, Release 10.5(1)*, available at: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/plm/10_5_1/userguide/CPLM_BK_UD1156AD_00_user-guide-rel-1051/CPLM_BK_UD1156AD_00_user-guide-rel-1051_chapter_010.html#CPLM_TK_G69E9158_00.
2. Configure Unity Connection with the PLM server to synchronize the products licensing information. For more information, see “Add Product Instance” section in “Operation” chapter of *Cisco Prime License Manager User Guide, Release 10.5(1)*, available at:

   http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/plm/10_5_1/userguide/CPLM_BK_UD1156AD_00_user-guide-rel-1051/CPLM_BK_UD1156AD_00_user-guide-rel-1051_chapter_010.html#CPLM_TK_AA222E94_00.

Note After completing the synchronization between Unity Connection and PLM, you can verify the license status from Cisco Unity Connection Administration> System Settings> Licenses. The Licenses page shows that the licenses in Unity Connection are no longer in **Demo** mode.

Status of Licenses

There is a transition in the Unity Connection license status after the synchronization between the PLM server and Unity Connection completes.

The different licensing modes in a Unity Connection server are:

- **Demo**: Unity Connection remains in the **Demonstration (Demo)** mode until it connects with the PLM server for the first time.

The system operates on demo licenses that expire in 60 days. Unity Connection must be connected to the PLM server to install sufficient feature licenses before the licenses expire.

- **Compliance**: After connecting Unity Connection to the PLM server and installing the respective feature licenses, the license status in Unity Connection changes to the **Compliance** mode.

  If the PLM server is configured for 50 users, Unity Connection can request licenses for less than or equal to 50 users to remain in the compliance mode.
- **Violation**: Unity Connection license status changes to the **Violation** mode either when the required number of licenses are not installed on PLM or the license limit exceeds for the required feature.

  The grace period for using the licenses is 60 days and to avoid license violation, you must install sufficient licenses or reduce the usage of licensed features.
- **Expire**: Unity Connection license status changes to the **Expire** mode if required licenses are not installed within the grace period of 60 days**.**

  In the **Expire** mode, creation of users with mailbox is not allowed. However, you can add or update any other configuration data on Unity Connection. You can also send or receive voicemails.

Note You must restart the Unity Connection server after obtaining and installing licenses. The license status on Unity Connection changes from “**Expire**” to “**Compliance**”.

Note When the license status of Unity Connection is “**Expire**”, the synchronization of users and call handler profiles from Unity Connection on the branch stops working. However, the voicemail and auto-attendant functionalities continue to work on the branch. For more information on the licensing requirements of a branch, see the “Compatibility Matrix, Software Requirements, and Licensing Requirements” chapter of the *Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) for Release 10.x,* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/srsv/guide/10xcucsrsvx/10xcucsrsv015.html#pgfId-1114809.

Note If multiple Unity Connection severs are configured with the same PLM server and license violation occurs for one of the Unity Connection server, then the license status of all Unity Connection servers changes to “**Violation**”. Similarly, if the license expiration occurs for one of the Unity Connection server, then the license status of all Unity Connection servers changes to “**Expire**”.

Licenses in Unity Connection Cluster

In a Unity Connection cluster, only the publisher server needs to be configured and connected with the PLM server to obtain the license status. When the publisher server stops functioning (for example, when it is shut down for maintenance), the subscriber server handles all the incoming calls for the cluster for a grace period of 60 days. However, if the publisher server fails to resume its functioning within 60 days, the license status in Unity Connection changes to “**Expire**” state.

Migrating Licenses

You need to make sure to migrate licenses in either of the following cases:

- Migrating Licenses from Cisco Unity, page 6-3
- Migrating Licenses from Unity Connection 8.6 and Earlier Releases, page 6-3

Note Before starting the migration or uploading the legacy license information, you must configure Unity Connection with the PLM server. For more information on configuring Unity Connection with the PLM server, see “Add Product Instance” section in “Operation” chapter of *Cisco Prime License Manager User Guide, Release 10.5(1)*, available at: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/plm/10_5_1/userguide/CPLM_BK_UD1156AD_00_user-guide-rel-1051/CPLM_BK_UD1156AD_00_user-guide-rel-1051_chapter_010.html#CPLM_TK_AA222E94_00.

Migrating Licenses from Cisco Unity

Unity Connection 7.x and later can use the existing license information in Cisco Unity when migrating from Cisco Unity 4.x or later to Unity Connection 7.x and later. This license information helps to enable the Unity Connection features.

For instructions on migrating from Cisco Unity 4.x or later to Unity Connection 10.x, see the Migrating from Cisco Unity 4.x and Later to Unity Connection 7.x and Later, page 5-4 section.

Migrating Licenses from Unity Connection 8.6 and Earlier Releases

You can use either of the following methods to migrate licenses from Unity Connection 8.6 and earlier releases when upgrading to later releases of Unity Connection:

- Using COBRAS Tool, page 6-3
- Using Upgrade Process, page 6-4

After uploading the legacy license information, Unity Connection is configured and synchronized with the PLM server. Once the synchronization is completed at the PLM server, the legacy license information for the new version of Unity Connection is sent to the PLM server for migration. Now, you can migrate licenses through the PLM server.

Warning **If you are upgrading from Unity Connection 8.6 or earlier to later releases, you must install 8.6 licenses before you perform the upgrade. This is because the installed license information considered as legacy license data is required to migrate licenses. After you upgrade to Unity Connection 9.x and later releases, you can not apply legacy licenses using the Prime License Manager.**

Using COBRAS Tool

To Migrate Licenses Using COBRAS tool

Step 1 Download and start the COBRAS export tool from:

http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Step 2 In the **License Details for Migration to Unity Connection 10.x and later** field, select **Backup Options** tab. To export the legacy license data from Cisco Unity, check the **License Details for migration to Unity Connection 10.x and later** check box.

Step 3 Enter the CLI credentials and select **OK**.

Step 4 Browse to the backup location for exporting the legacy license data in the **Backup Destination** tab.

Step 5 Select the **Export Data** tab to export the legacy license data.

Note Similarly, you can use COBRAS import tool to import the backup data to the upgraded version.

Using Upgrade Process

If you are upgrading from Unity Connection 8.6 and later releases to Unity Connection 9.x and later releases, the legacy license information of the earlier release is uploaded to the upgraded release database. After the completion of upgrade process, the new upgraded version of Unity Connection needs to be synchronized with the PLM server. See the "Installing Licenses on the PLM server, page 6-1 section.

Viewing Reports for Licenses

To view the reports for the licenses associated with the licensed features, navigate to Cisco Unity Connection Administration, expand **System Settings** and select **Licenses**. The Licenses page shows the license report that includes the following information:

- **Status**: Shows the license status, hostname or IP address of the PLM server, the last connectivity time, and the last compliance time of Unity Connection with the PLM server.
- **License Usage**: Shows the usage of licensed features on the Unity Connection server. For features that are licensed for a number of seats, the report displays the number of used seats.

Viewing the License Usage

To View the License Usage on Unity Connection

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand **System Settings** and select **Licenses**.

Step 3 On the Licenses page, from the **License Usage** menu, the license usage for the Unity Connection server is displayed in the "**Current usage**" column.

Viewing the Last Connectivity Time with the PLM Server

To View the Last Connectivity Time of Unity Connection with the PLM Server

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand **System Settings** and select **Licenses**.

Step 3 On the Licenses page, from the **Status** menu, the value of the **Last Connectivity Time of Unity Connection with the PLM server** is displayed.

Note The value of the **Last Connectivity Time** with the PLM Server will be in **Coordinated Universal Time (UTC)** time zone.

Viewing the Hostname or IP Address of the Connected PLM Server

To View the Hostname or IP Address of the Connected PLM Server

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand **System Settings** and select **Licenses**.

Step 3 On the Licenses page, from the **Status** menu**,** the hostname or IP address of the connected PLM server is displayed.

Viewing the Last Compliance Time

To View the Last Compliance Time on the Unity Connection Server

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 Expand **System Settings** and select **Licenses**.

Step 3 On the Licenses page, from the **Status** menu, the value of the last compliance time of Unity Connection with the PLM server is displayed.

Note The value of the **Last Compliance Time** will be in **Coordinated Universal Time (UTC)** time zone.

License Parameters for Unity Connection Features

Table 6-1 License Parameters for Unity Connection Features

License Parameter	Feature	Description
CUC_BasicMessaging	Total number of voicemail users.	Specifies the maximum number of voice mail users configured in Unity Connection.
CUC_EnhancedMessaging	Total number of enhanced messaging users.	Specifies the maximum number of Unity Connection SRSV users configured on Unity Connection. The Unity Connection SRSV users are reflected under this tag only when the branch is active.
CUC_SpeechView	Total number of speech view standard users.	Specifies the maximum number of Speech view Standard users configured in Unity Connection.
CUC_SpeechViewPro	Total number of speech view professional users.	Specifies the maximum number of Speech view Professional users configured in Unity Connection.
CUC_SpeechConnectPort	Total number of speech connect ports.	Specifies the maximum number of Speech Connect calls configured in Unity Connection.